Individual Secrecy for the Broadcast Channel

Yanling Chen, O. Ozan Koyluoglu, and Aydin Sezgin

Abstract

This paper studies the problem of secure communication over broadcast channels under the *individual* secrecy constraints. That is, the transmitter wants to send two independent messages to two legitimate receivers in the presence of an eavesdropper, while keeping the eavesdropper ignorant of *each* message (i.e., the information leakage from *each* message to the eavesdropper is made vanishing). Building upon Carleial-Hellman's secrecy coding, Wyner's secrecy coding, the frameworks of superposition coding and Marton's coding together with techniques such as rate splitting and indirect decoding, achievable rate regions are developed. The proposed regions are compared with those satisfying joint secrecy and without secrecy constraints, and the individual secrecy capacity regions for special cases are characterized. In particular, capacity region for the deterministic case is established, and for the Gaussian model, a constant gap (i.e., 0.5 bits within the individual secrecy capacity region) result is obtained. Overall, when compared with the joint secrecy constraint, the results allow for trading-off secrecy level and throughput in the system.

I. Introduction

A. Background

The broadcast channel (BC) involves the simultaneous communication of information from one transmitter to multiple receivers. The broadcast nature makes the communication susceptible to eavesdropping. Therefore, it is desirable to offer a reliable communication with a certain level of security guarantee, especially to ensure that sensitive information is protected from unauthorized parties.

The most fundamental model of the BC is the two-receiver BC with two independent messages. This basic model and its extensions with or without an external eavesdropper have been well studied [1]–[10]. However, capacity regions have still remained open for the basic model (i.e., two independent private messages are dedicated to two legitimate receivers, respectively), and its extension with an external eavesdropper subject to a *joint* secrecy constraint (whereby the information leakage from *both* messages to the eavesdropper is made vanishing). Nevertheless, in case that the channels to all the receivers (and the eavesdropper) fulfill a certain degradation order, the capacity regions are characterized and superposition coding is shown to be optimal in both settings [1]–[3], [7].

This paper was presented in part at IEEE International Symposium on Information Theory, Hong Kong, Jun. 2015.

Y. Chen and A. Sezgin are with the Institute of Digital Communication Systems, Ruhr University Bochum, Germany (e-mail: yanling.chen-q5g@rub.de, aydin.sezgin@rub.de). O. O. Koyluoglu is with the Department of Electrical and Computer Engineering, The University of Arizona, Tucson, AZ 85721, USA (e-mail: ozan@email.arizona.edu).

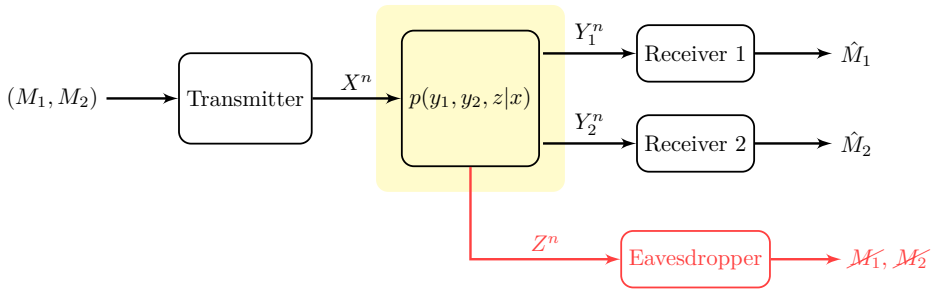


Fig. 1: BC with an external eavesdropper.

In this paper, we primarily focus on the problem of secure communication over the BC subject to the *individual* secrecy constraint. The channel model is shown in Fig. 1. Differently from the joint secrecy constraint, here one aims to minimize the information leakage from *each* message to the eavesdropper. Remarkably, the joint secrecy constraint offers a higher secrecy level from the system design perspective (but unfortunately not always affordable [11]), while the individual secrecy constraint could provide an acceptable security strength from the end user's point of view with potential gains in increasing transmission rates. Therefore, the notion of individual secrecy allows for trading-off of the throughput and secrecy level.

To ensure a pre-specified secrecy level, there are popular cryptographic means as demonstrated by Shannon [12] that rely on the secret keys shared only between the transmitter and the intended receiver in advance of the communication. Another well-known information-theoretic means is by Wyner's secrecy coding introduced in [13], where he proposed the model of the wiretap channel. The main idea is to explore the advantage of the channel of the legitimate receiver against a *degraded* eavesdropper by the means of trading rate for secrecy. More specifically, sufficient randomness is added to the codeword in order to keep the eavesdropper totally ignorant of the transmitted message. Later on, a sharper result for the wiretap channel is obtained by Csiszár and Körner [14] by considering a general setup of transmitting the common and confidential messages over a channel where the eavesdropper's channel is not necessarily a degraded version of the channel of the legitimate receiver.

Another secrecy coding method that has not attracted enough attention, but plays an important role in this paper for the purpose of individual secrecy, is a coding technique introduced by Carleial and Hellman in [15] for a special case of the wiretap channel, where the channel to the legitimate receiver is noiseless and the eavesdropper's channel is a binary symmetric channel (BSC) with cross probability p. It is demonstrated that it is possible to send message (of length n and divided into n/l pieces each with l bits) at capacity (i.e., rate 1) over the main channel while still keeping the eavesdropper totally ignorant of *each* piece of the message provided that $nh(p) \geq l$. The main observation is that message pieces can hide each other without a need of additional randomness (under this weaker secrecy notion). In this paper, we generalize this coding idea to the broadcast channel scenarios and refer to it as Carleial-Hellman's secrecy coding. The goal remains

the same, i.e., to keep the eavesdropper totally ignorant of each piece of the messages. Differently from the original proposal in [15], the channel is not restricted to be noiseless or BSC, each piece of the messages are destined at different receivers, and each piece of the messages are not necessarily of the same length.

B. Contributions

In this paper, we consider the problem of secure communication over the broadcast channel, where the transmitter wants to send two independent messages to two legitimate receivers in the presence of an external eavesdropper. (See Fig. 1.) In the following, we summarize the main contributions of the paper:

- The linear deterministic model is studied and corresponding capacity regions under different secrecy constraints are characterized. Study of this specific model provides insights into the capacity regions for the Gaussian case under different secrecy constraints, especially in the high SNR regime.
- To investigate the fundamental limits of communication under the individual secrecy constraints, constructions building upon Carleial-Hellman's secrecy coding, Wyner's secrecy coding, superposition coding, and Marton's coding, rate splitting and indirect decoding are proposed for the general discrete memoryless broadcast channel (DM-BC) with an external eavesdropper.
  - First construction, referred to as the primitive approach, utilizes Carleial-Hellman's secrecy coding in the sense that it regards one message as (partial) randomness for ensuring the individual secrecy of the other. This approach is shown to be optimal if the channels to both legitimate receivers are statistically identical.
  - The primitive approach is suboptimal for the case when one legitimate receiver's channel is less noisy than the other. To further benefit from the channel advantage of the strong receiver, we propose the superposition coding scheme by taking the primitive approach as the cloud coding layer, and adding to it another satellite coding layer. Differently from the cloud layer that employs Carleial-Hellman's secrecy coding, we employ Wyner's secrecy coding in the satellite layer to ensure the secrecy of the additional message to the strong receiver. This approach is shown to be optimal for the case of a *comparable* eavesdropper (compared to the weak legitimate receiver); and the case that the weak legitimate receiver has a *deterministic* channel and the eavesdropper's channel is a degraded version of it.
  - Considering the general case where there may not be less noisiness order between the channels to the legitimate receivers, we devise a coding scheme by utilizing Marton's coding. The idea is to explore the advantage of rate splitting at the encoding phase (with introduction of jointly distributed satellite codewords that carry independent message pieces intended for each legitimate receiver); and recovering the individual satellite codewords at the decoding phase. As a result, a general achievable individual secrecy rate region is established, which includes regions obtained by the primitive approach and superposition coding approach as special cases.

- Following the (Marton's) coding scheme proposed and appropriately modifying its analysis for secrecy, an achievable *joint secrecy* rate region is established. This region is contrasted with the previous regions reported in the literature.
- Gaussian model is studied, and a constant gap result (i.e., 0.5 bits within the individual secrecy capacity region) is obtained. In particular, the individual secrecy capacity region is characterized for the *comparable* eavesdropper case (defined by satisfying $\sigma_2^2 \leq \sigma_e^2 \leq 2\sigma_2^2$ for the noise variances of weaker receiver and eavesdropper). To visualize the impact of different secrecy constraints on the fundamental limits, comparisons are made among the capacity regions of Gaussian-BC without secrecy constraint, and with individual and joint secrecy constraints.

C. Related Work

The broadcast channel involves the simultaneous communication of information from one transmitter to multiple receivers. Generally speaking, the information may be independent or nested. For the general two-receiver BC with two independent messages, the capacity region is yet unknown. Nevertheless, if one receiver's channel is degraded to the other, then the capacity region is fully characterized and it is shown that superposition coding is optimal [1]–[3]. In general, the best known achievable rate region is obtained by Marton's coding in [5]. For the BC with nested information, one instance is the two-receiver BC with one common and two private messages. The model was first introduced by Körner and Marton in [16], and the general capacity region still remains as unknown. Nevertheless, in [16], the capacity region was established for the two-receiver BC with degraded message sets (i.e., when one of the private message has rate zero). In [8], Nair and El Gamal extended the two-receiver BC with degraded message sets to the three-receiver case. In particular, they studied the specific case where one common message is sent to all three receivers, while one private message is sent to only one receiver. They proposed a new coding referred to as *indirect decoding* and showed that the resulting region of this technique is strictly greater than the straightforward extension of the Körner-Marton region for this scenario. Other studies on BC with different message degradation setups include [8], [17], [18], see also [19] for an overview.

Due to the very broadcast nature of the communications, adversaries may overhear the transmissions, resulting in data leakage. Secure broadcasting refers to the situation where one transmitter communicates with several legitimate receivers in the presence of an adversary (external eavesdropper). Inspired by the pioneering works [12]–[14] that studied the point-to-point secure communication, there has been a growing body of literature that investigate the problem of secure broadcasting with two or more receivers [7], [9]–[11], [20]–[22].

The *joint* secrecy capacity region for some special cases are established in [7], especially for certain degradation orders among the channels. The results of [7] were extended to the Gaussian scenario in [20]; and to the degraded compound multi-receiver broadcast channel in [21]. Moreover, [10] studied the BC with two receivers and one eavesdropper, where the transmitter wants to transmit a pair of public and

confidential messages to each legitimate receiver, and established the joint secrecy capacity for the degraded channels and when the confidential message to the strong receiver is absent. Nested information transmission with secrecy constraints were considered in [9]. This work investigated the transmission of one common and one confidential message over a BC with two receivers and one eavesdropper, where the common message is to be delivered to both legitimate receivers and the eavesdropper, whilst the confidential message is to be delivered to both legitimate receivers but kept secret from the eavesdropper. A general achievable rate region is derived, and the secrecy capacity is established when the two legitimate receivers are less noisy than the eavesdropper. In some cases, the indirect decoding is shown to provide an inner bound that is strictly larger than the direct extension of Csiszár and Köner's approach. Another relevant direction is the BC with privacy constraints [23]–[25]. The model was first introduced by Cai and Lam in [23], where each receiver not only should correctly decode its own message but also obtain no information about the message of the other receiver. In [23], the authors focused on the deterministic BC and established its capacity region. The general inner and outer bound were established later in [24]. Recently, the authors of [25] considered an extension of this two-receiver BC model (i.e., BC with one common and two private messages, where each private message should satisfy a pre-specified constraint measured at the other receiver). The capacity regions are determined for semi-deterministic and physically degraded BCs and the BC with a degraded message set.

Consider secure broadcasting when there is no common message or public message involved. In case that only one confidential message is to be delivered, then at the eavesdropper both the *joint* secrecy constraint and the *individual* secrecy constraint reduce to the same. However, in case that independent confidential massages are to be delivered to multi-receivers, the two secrecy constraints can be quite different. By definition, the individual secrecy constraint is weaker than the joint one. The joint secrecy, however, is not always affordable [11], and satisfying the individual secrecy can provide positive rates under these scenarios. Especially this secrecy notion offers an acceptable security level (that keeps each message to individually leak negligible information to eavesdropper), while potentially improving transmission efficiency. In [15], this notion of secrecy is analyzed for the point-to-point channel, and message pieces can be made individually secret without any degradation of channel capacity. In [26], we considered the problem of achieving individual secrecy over a BC with receiver side information (where each receiver has the desired message of the other receiver as side information). The individual secrecy rate region results are obtained for general models with full characterization for some special cases (e.g.: of either a strong or weak eavesdropper compared to both legitimate receivers). More detailed discussion and results on this model are presented in [27]. The joint secrecy counterpart for this problem is studied in [28] and in [29], where the latter work also considers nested information models (referred to as cognitive messages therein) under both individual and joint secrecy constraints. We remark that, in these models with side information, the readily available message of the other user can serve as secret key (in one-time pad fashion). And, this coding strategy satisfies the individual secrecy condition as the analysis for secrecy is performed per message basis (i.e., in an individual fashion),

where each analysis considers the other message as secret key.

In this work, the problem of secure broadcasting subject to the *individual* secrecy constraints is analyzed. Wyner's secrecy coding continues to play an important role. Nevertheless, we find that Carleial-Hellman's secrecy coding is also essential for the individual secrecy setting. (As compared to prior works, the side information is absent at receivers in this model). Using the insights gained from the previous studies, we construct a superposition coding approach for special class of BCs (e.g., for certain less noisiness/degradation orders) and utilize Marton's coding for the general case. Overall, the results here establishes a comparison between different secrecy notions in BCs, in particular comparing BC with no secrecy constraints, BC with joint secrecy constraints with that of individual secrecy constraints.

D. Notations and Organization

In this paper, we follow the convention to denote random variables by capital letters, their realizations by the corresponding lower case letters and their images (or ranges) by calligraphic letters. In addition, we use X^n to denote the sequence of variables $(X_1, \cdots, X_n)$, where X_i is the i-th variable in the sequence, X^{i-1} the sequence $(X_1, \cdots, X^{i-1})$ and X_{i+1}^n the sequence $(X_{i+1}, \cdots, X_n)$. $\mathcal{R}_+$ is used to denote the set of nonnegative real numbers. $[a:b]$ is used to represent the set of natural numbers between a and b. We use shorthands $[a]^+ = \max\{0, a\}$, and $C(x) = \frac{1}{2}\log_2(1+x)$.

The rest of the paper is organized as follows. Section II introduces the system model, and Section III provides the results for the determistic case. Main results for the discrete memoryless model is given in Section IV, and for the Gaussian case in Section V. Section VI concludes the paper. To enhance the flow, details are relegated to appendices.

II. System model

Consider a DM-BC with two legitimate receivers and one passive eavesdropper defined by $p(y_1, y_2, z|x)$. The model is shown in Fig. 1. The transmitter aims to send messages m_1, m_2 to receiver $1, 2$, respectively. Suppose that x^n is the channel input, whilst y_1^n (at receiver 1), y_2^n (at receiver 2) and z^n (at eavesdropper), are the channel outputs. By the *discrete memoryless* nature of the channel, we have

$$p(y_1^n, y_2^n, z^n|x^n) = \prod_{i=1}^{n} p(y_{1i}, y_{2i}, z_i|x_i). \tag{1}$$

A $(2^{nR_1}, 2^{nR_2}, n)$ secrecy code for the DM-BC $p(y_1, y_2, z|x)$ consists of

- Two message sets $\mathcal{M}_1$ and $\mathcal{M}_2$, where $m_1 \in \mathcal{M}_1 = [1 : 2^{nR_1}]$ and $m_2 \in \mathcal{M}_2 = [1 : 2^{nR_2}]$;
- a (randomized) encoder that assigns a codeword x^n to each message pair (m_1, m_2); and
- two decoders, where decoder i (at legitimate receiver i) assigns an estimate of m_i, say $\hat{m}_i$, or an error to each received sequence y_i^n.

The messages M_1, M_2 are assumed to be uniformly distributed over their corresponding message sets. Therefore, we have $R_i = \frac{1}{n}H(M_i)$, for $i = 1, 2$. Associated with the $(2^{nR_1}, 2^{nR_2}, n)$ secrecy code, the *individual*

information leakage rates are defined as $R_{L,i} = \frac{1}{n} I(M_i; Z^n)$ for $i = 1, 2$, while the *joint* information leakage rate is defined as $R_L = \frac{1}{n} I(M_1, M_2; Z^n)$.

Denote the *average probability of decoding error* at receiver i as $P_{e,i}^n = \Pr(M_i \neq \hat{M}_i)$. The rate pair (R_1, R_2) is said to be *individual secrecy achievable*, if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes such that

$$P_{e,i}^n \leq \epsilon_n, \quad \text{for } i = 1, 2 \tag{2}$$

$$R_{L,i} \leq \tau_n, \quad \text{for } i = 1, 2 \tag{3}$$

$$\lim_{n\to\infty} \epsilon_n = 0 \quad \text{and} \quad \lim_{n\to\infty} \tau_n = 0. \tag{4}$$

Note that, (3) corresponds to the *individual* secrecy constraints. If the coding schemes fulfill (2), (4) and

$$R_L \leq \tau_n, \tag{5}$$

then the rate pair (R_1, R_2) is said to be achievable under *joint secrecy*. Clearly, the joint secrecy constraint (5) implies the individual secrecy (3), and hence the jointly secret achievable rate pairs are by definition achievable as individually secret.

Two important classes of DM-BC are the classes of *less noisy* channels and the class of *degraded* channels, and will be also addressed in this paper. Given a DM-BC that is defined by $p(y_1, y_2, z|x)$, formally, Y is said to be *less noisy* than Z, if

$$I(U; Y) \geq I(U; Z) \tag{6}$$

holds for any random variable U such that $U \to X \to (Y, Z)$ forms a Markov chain. And, Z is said to be a *physically degraded* version of Y, if

$$p(y, z|x) = p(y|x)p(z|y), \tag{7}$$

i.e., $X \to Y \to Z$ forms a Markov chain for any input random variable X. More generally, Z is said to be a *stochastically degraded* (or simply *degraded*) version of Y, if there exists a random variable $\tilde{Y}$ such that $\tilde{Y}$ has the same conditional probability mass function as Y (given X), and $X \to \tilde{Y} \to Z$ forms a Markov chain.

III. A special instance: linear deterministic case

Let us first take a look at the deterministic broadcast channel. In this model, the received signals at the legitimate receivers and the eavesdropper are given by

$$Y_1 = D^{q-n_1} X; \tag{8}$$

$$Y_2 = D^{q-n_2} X; \tag{9}$$

$$Z = D^{q-n_e} X; \tag{10}$$

where X is the binary input vector of length $q = \max\{n_1, n_2, n_e\}$; D is the $q \times q$ down-shift matrix; n_1, n_2 and n_e are the integer channel gains of the channels from the transmitter to receiver 1, receiver 2, and the

eavesdropper, respectively. Without loss of generality, we assume that $n_1 \geq n_2$. Under this assumption, Y_2 is a degraded version of Y_1 according to the channel definition. In this case, we have the following theorem:

Theorem 1. *The individual secrecy capacity region of the linear deterministic broadcast channel with an external eavesdropper is the set of the rate pairs* $(R_1, R_2) \in \mathcal{R}_+^2$ *defined by*

$$\begin{aligned} R_1 &\leq [n_1 - n_e]^+; \\ R_2 &\leq [n_2 - n_e]^+; \\ R_1 + R_2 &\leq n_1. \end{aligned} \tag{11}$$

Proof: See Appendix A. ■

Remark: Note that in our achievability schemes, the elements of the input vector X are i.i.d. Bern($\frac{1}{2}$) in all scenarios. That is, Bern($\frac{1}{2}$) serves as an optimal input distribution to achieve the individual secrecy capacity. Nevertheless, this universal choice is not the only optimal one. As an alternative, one can simply zero-pad those $r(k)$ bits, where random bits are set in our proposals.

Similarly one can derive the following theorems for the linear deterministic broadcast channel: without secrecy constraint, and under the joint secrecy constraint.

Theorem 2. *The capacity region of the linear deterministic broadcast channel is the set of the rate pairs* $(R_1, R_2) \in \mathcal{R}_+^2$ *defined by*

$$\begin{aligned} R_2 &\leq n_2; \\ R_1 + R_2 &\leq n_1. \end{aligned} \tag{12}$$

Proof: Under the assumption that $n_1 \geq n_2$, (12) follows directly from the capacity region of the degraded BC [2], [3], [19]. ■

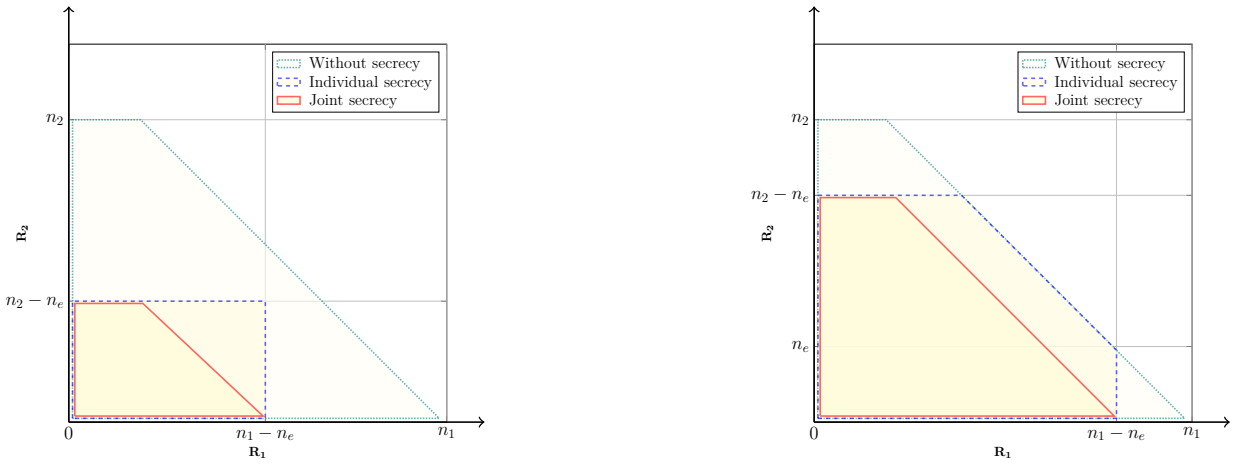
Theorem 3. *The joint secrecy capacity region of the linear deterministic broadcast channel with an external eavesdropper is the set of the rate pairs* $(R_1, R_2) \in \mathcal{R}_+^2$ *defined by*

$$\begin{aligned} R_2 &\leq [n_2 - n_e]^+; \\ R_1 + R_2 &\leq [n_1 - n_e]^+. \end{aligned} \tag{13}$$

Proof: Under the assumption that $n_1 \geq n_2$, we consider the following different scenarios:

- In case of a more noisy eavesdropper, i.e., as $q = n_1 \geq n_2 \geq n_e$, (13) follows directly from the joint secrecy capacity region of the degraded BC [7, Corollary 2];
- In other cases (i.e., as $q = n_1 \geq n_e \geq n_2$, or as $q = n_e \geq n_1 \geq n_2$), the channel degenerates to a degraded wiretap channel as $R_2 = 0$ or $R_1 = 0$. As a direct consequence, its joint secrecy capacity region (13) reduces to the ones for the wiretap channel [13], [14].

■



(a) $0 < n_2 - n_e \leq n_e$ (b) $n_2 - n_e > n_e$

Fig. 2: Capacity regions of deterministic BC.

For the linear deterministic BC, we note that non-degenerate individual/joint secrecy rate regions are possible only for the case as $n_1 \geq n_2 \geq n_e$. Its capacity regions under different secrecy constraints are depicted in Fig. 2.

1) Without any secrecy constraints, the capacity region is a *triangle with one missing corner*, where the triangle is caused by the non-negativity of the rates and the upper bound on the sum rate (since two legitimate receivers share the same transmission channel); while the missing corner is due to the fact that the transmission rate R_2 is upper bounded by its channel capacity (i.e., n_2).
2) Under individual secrecy constraint:
   - The capacity region is a *rectangle* in case of $n_e \leq n_2 \leq 2n_e$. In this case, the transmitter could send messages to both legitimate receivers up to their individual secrecy capacity ($n_1 - n_e$, $n_2 - n_e$ bits, respectively) in one channel use (up to n_1 bits).
   - The capacity region is a *rectangle with one missing corner* in case of $n_2 > 2n_e$. In this case, the transmitter could not send secret messages to both legitimate receivers up to their individual secrecy capacity ($n_1 - n_e$, $n_2 - n_e$ bits, respectively) in one channel use (up to n_1 bits).

   Note that in both cases, receiver 1 could decode the message to receiver 2 (due to the degradedness of the channel). Thus m_2 could be regarded as side information available at receiver 1. This advantage could be explored in the transmission phase where part of m_1 could be secured via one-time pad [12] with m_2 while the rest via Wyner's secrecy coding [13], [14]. Besides, compared to the capacity region without any secrecy constraints, there is n_e bits loss for the maximal transmission rates R_1, R_2, respectively, due to the individual secrecy constraint.
3) Under joint secrecy constraint, the capacity region is a *triangle with one missing corner*. Compared to

the capacity region without any secrecy constraints, there is not only a loss of n_e bits for the maximal transmission rates R_1, R_2, respectively, (as under the individual secrecy constraint), but also n_e bits loss for the sum rate $R_1 + R_2$. This additional loss on the sum rate $R_1 + R_2$ is due to the fundamental difference between the *joint* secrecy (3) and the *individual* secrecy (5) constraints.

IV. DM-BC with an external eavesdropper

In this section, we investigate the DM-BC with an external eavesdropper where the individual secrecy constraint is imposed. For this channel model, similar to the discussion in [11], positive rate pairs (i.e., $(R_1, R_2) \in \mathcal{R}_+^2$) are not possible, if the eavesdropper's channel is less noisy than either legitimate receiver's channel.

A. Primitive approach

A primitive approach is to utilize the secrecy coding while regarding one message as (partial) randomness for ensuring the individual secrecy of the other. The idea is similar to Carleial-Hellman's secrecy coding [15], in the sense that the eavesdropper should be kept totally ignorant of each message individually. Differently from [15], here two messages are aimed at different destinations. As a direct consequence (if only such a secrecy coding is employed), the sum rate is limited by the worse channel to the legitimate receivers.

Theorem 4. *For the DM-BC with an external eavesdropper, an achievable individual secrecy rate region is given by the union of the rate pairs $(R_1, R_2) \in \mathcal{R}_+^2$ satisfying*

$$\begin{aligned} R_1 + R_2 &\leq \min\{I(U;Y_1), I(U;Y_2)\} \\ \max\{R_1, R_2\} &\leq \min\{I(U;Y_1), I(U;Y_2)\} - I(U;Z) \end{aligned} \tag{14}$$

over all $p(u)p(x|u)$.

Proof: See Appendix B. ∎

An intuitive interpretation of the achievable region in (14) is as follows. The first inequality in (14) imposes condition on the sum rate $R_1 + R_2$, which is due to decodability constraints at both legitimate receivers. While, the second inequality imposes condition on both individual rates, i.e., R_1, R_2. This follows from the spirit of Carleial-Hellman's secrecy coding for the purpose of individual secrecy. That is, for each message, at least $I(U;Z)$ randomness is needed to keep it secret from the eavesdropper.

Note that (14) can be rewritten in a compact form as follows:

$$\max\{R_1 + R_2, \max\{R_1, R_2\} + I(U;Z)\} \leq \min\{I(U;Y_1), I(U;Y_2)\}. \tag{15}$$

Remarkably, in the case that the left-hand side (LHS) of (15) equals to $R_1 + R_2$, we have $R_1, R_2 \geq I(U;Z)$ and it implies that U^n codewords are fully employed to carry the individually secured messages. (That is, each message plays also the role of randomness to ensure the secrecy of the other and no additional

randomness is needed since $R_i = H(M_i)/n \geq I(U;Z)$). In the other case, additional randomness is needed to ensure the individual secrecy of both messages.

This primitive approach is optimal if the channels to both legitimate receivers are statistically identical. However, it is not optimal in general, since both rates are limited by the worse legitimate receiver. For instance, suppose that Y_1 is strictly less noisy than $Y_2 = Z$ (i.e., $I(U;Y_1) > I(U;Y_2) = I(U;Z)$ for any $p(u,x)$.) Then, employing this primitive approach will convey no secret information to either legitimate receiver. On the other hand, positive secret rate (i.e., $R_1 \in \mathcal{R}_+$) is clearly possible by ignoring the worse legitimate receiver, and employing Wyner's secrecy coding for the resulting wiretap channel [13].

In order to further employ the channel advantage of the strong legitimate receiver against the eavesdropper, we propose the following superposition coding approach.

B. Superposition coding approach

It is well-known that superposition coding is optimal for a degraded broadcast channel where $X \to Y_1 \to Y_2$ forms a Markov chain, wherein the weak receiver could decode the cloud center whilst the strong receiver could decode both the cloud center and satellite codewords [19]. Such a coding scheme explores the channel advantage of the stronger legitimate receiver, so that the messages conveyed are not bounded by the worse channel. Utilizing such a superposition coding framework with embedded Carleial-Hellman's secrecy coding in the layer of cloud codeword and Wyner's secrecy coding in the layer of the satellite codeword, we have the following achievable individual secrecy rate region.

Theorem 5. *For the DM-BC with an external eavesdropper, an achievable individual secrecy rate region is given by the union of rate pairs $(R_1, R_2) \in \mathcal{R}_+^2$ with $R_1 = R_{1s} + R_{1k}$, where $(R_{1s}, R_{1k}) \in \mathcal{R}_+^2$, that satisfies*

$$\begin{aligned} R_k \leq & I(U;Y_2) \\ R_{1s} \leq & I(V_1;Y_1|U) - I(V_1;Z|U) \\ R_k + R_{1s} \leq & I(U,V_1;Y_1) - I(V_1;Z|U) \end{aligned} \tag{16}$$

with

$$R_k = \max\left\{R_{1k} + R_2, \max\{R_{1k}, R_2\} + I(U;Z)\right\} \tag{17}$$

Or, equivalently in terms of (R_1, R_2),

$$\begin{aligned} R_2 &\leq I(U;Y_2) - I(U;Z), \\ R_1 &\leq [I(V;Y_1|U) - I(V;Z|U)]^+ + I(U;Y_2) - I(U;Z) \\ \max\{R_1, R_2\} &\leq [I(V;Y_1|U) - I(V;Z|U)]^+ + I(U;Y_1) - I(U;Z) \\ R_1 + R_2 &\leq [I(V;Y_1|U) - I(V;Z|U)]^+ + \min\{I(U;Y_1), I(U;Y_2)\} \end{aligned} \tag{18}$$

over all $p(u)p(v|u)p(x|v)$.

Proof: See Appendix C. ■

Our proposed superposition coding scheme consists of two coding layers. In particular, m_2 and part of m_1 (say m_{1k}) are conveyed via the first layer by employing Carleial-Hellman's secrecy coding, where each message not only plays the role of being the information to be destined to a different legitimate but also the (partial) randomness for the other message to be (individually) secured from the eavesdropper. In the second layer, extra information is conveyed via the satellite codewords to one of the receivers (assumed receiver 1 here), in which an extra part of the message (say m_{1s}) is secured by employing Wyner's secrecy coding. Applying this superposition coding with embedded different secrecy coding in two coding layers, one readily achieves the individual secrecy rate region as provided in Theorem 5. We note that Theorem 5 does not require any less noisiness order between the legitimate receivers.

We note that, the first inequality (i.e., the bound on R_k) in (16) is contributed by the cloud codewords in the first coding layer for (m_{1k}, m_2) and the fact that the cloud codewords will be decoded at receiver 2; whilst the second inequality in (16) gives the extra secret information (if any) for the receiver 1, i.e., achievable R_{1s}, that is carried by the satellite codewords in the second coding layer for m_{1s} (just as for a classical wiretap channel); the third inequality in (16) comes from the fact that receiver 1 uses indirect decoding to decode $m_1 = (m_{1k}, m_{1s})$ and there is a rate loss of $I(V_1; Z|U)$ for the sake of the individual secrecy of the message.

Such a superposition coding scheme explores not only the advantage of Carleial-Hellman's secrecy coding for the purpose of individual secrecy that is discussed in the primitive approach, but also the channel advantage of the strong receiver (since he/she may decode both the cloud and satellite codewords) to obtain extra gains in the secret rate, i.e., R_{1s}. Assuming that Y_1 is less noisy than Y_2, Theorem 5 reduces to the following.

Corollary 6. *For the DM-BC with an external eavesdropper such that Y_1 is less noisy than Y_2, an achievable individual secrecy rate region is given by the union of rate pairs $(R_1, R_2) \in \mathcal{R}_+^2$ with $R_1 = R_{1s} + R_{1k}$, where $(R_{1s}, R_{1k}) \in \mathcal{R}_+^2$, that satisfies*

$$\begin{aligned} R_k &\leq I(U; Y_2) \\ R_{1s} &\leq I(V; Y_1|U) - I(V; Z|U) \end{aligned} \tag{19}$$

with R_k as defined in (17)*. Or, equivalently in terms of (R_1, R_2),*

$$\begin{aligned} R_2 &\leq I(U; Y_2) - I(U; Z), \\ R_1 &\leq [I(V; Y_1|U) - I(V; Z|U)]^+ + I(U; Y_2) - I(U; Z) \\ R_1 + R_2 &\leq [I(V; Y_1|U) - I(V; Z|U)]^+ + I(U; Y_2) \end{aligned} \tag{20}$$

over all $p(u)p(v|u)p(x|v)$.

Remark: We have the following interesting observations:

- Setting $U = \emptyset$, i.e., $R_2 = R_{1k} = 0$, the region (19) of $R_1 = R_{1s}$ coincides with the secrecy capacity region of the wiretap channel [13], [14];

- If we let $Z = \emptyset$, and $R_{1k} = 0$, the region (19) reduces to the capacity region of the degraded broadcast channel, as established in [1]–[3].
- If we let $R_{1k} = 0$, then the region (19) reduces to the joint secrecy capacity region of the degraded broadcast channel [7], [30]. The proof follows when the individual secrecy constraints (i.e., (3)), are replaced with joint secrecy constraints (i.e., (5)), for which the resulting coding scheme, as shown in [7], [30], achieves the joint secrecy capacity region for the degraded broadcast channel.

Theorem 7. *For the DM-BC with an external eavesdropper such that*

1) *Y_1 is less noisy than Y_2;*
2) *Y_2 is a deterministic function of X; and*
3) *Z is a degraded version of Y_2,*

the individual secrecy capacity region is given by the union of rate pairs $(R_1, R_2) \in \mathcal{R}_+^2$ satisfying

$$\begin{aligned} R_2 &\leq H(Y_2|Z) \\ R_1 &\leq I(X;Y_1) - I(X;Z) \\ R_1 + R_2 &\leq I(X;Y_1) \end{aligned} \tag{21}$$

over all $p(x)$.

Proof: The achievability follows directly from Corollary 6 by taking $U = Y_2$ and $V = X$. (Note that in case that Y_2 is a deterministic function of X, and $X \to Y_2 \to Z$ forms a Markov chain, we have $I(X;Z|Y_2) = 0$, $H(Y_2) = I(X;Y_2)$ and $I(Y_2;Z) = I(X;Z)$.) For the converse, the first two inequalities for R_1, R_2, respectively, follow directly from the classical results of wiretap channel by simply ignoring the other legitimate receiver [14]. And, the last inequality follows directly from the upper bound on the sum rate for the relaxed setting of without any secrecy constraints. ■

In the following, we provide an upper bound on the individual secrecy capacity region, that will be used to derive a special case secrecy capacity result in the sequel.

Theorem 8. *For the DM-BC with an external eavesdropper such that*

1) *Y_2 is a degraded version of Y_1; and*
2) *Y_2 is less noisy than Z,*

the individual secrecy capacity region is upper bounded by the union of rate pairs $(R_1, R_2) \in \mathcal{R}_+^2$ satisfying

$$\begin{aligned} R_2 &\leq I(U;Y_2) - I(U;Z) \\ R_1 &\leq I(V;Y_1|U) - I(V;Z|U) + I(U;Y_2) - I(U;Z) \\ R_1 + R_2 &\leq I(V;Y_1|U) + I(U;Y_2) \end{aligned} \tag{22}$$

over all $p(u)p(v|u)p(x|v)$.

Proof: See Appendix D. ■

Theorem 9. *For the DM-BC with an external eavesdropper such that*

1) *Y_2 is a degraded version of Y_1;*
2) *Y_2 is less noisy than Z; and*
3) *$I(U;Z) \leq I(U;Y_2) \leq 2I(U;Z)$ holds for any $p(u,v,x)$,*

the individual secrecy capacity region is given by the union of rate pairs $(R_1, R_2) \in \mathcal{R}_+^2$ satisfying

$$\begin{aligned} R_2 &\leq I(U;Y_2) - I(U;Z), \\ R_1 &\leq I(V;Y_1|U) - I(V;Z|U) + I(U;Y_2) - I(U;Z) \end{aligned} \tag{23}$$

over all $p(u)p(v|u)p(x|v)$.

Proof: The achievability follows from Corollary 6 when the channel fulfills the conditions 1), 2) and 3). In particular, the sum rate condition becomes redundant due to condition 3). Since the derived region in this case coincides with the upper bound in Theorem 8, it gives the individual secrecy capacity region. ■

Remark: One can recall the linear deterministic BC with an external eavesdropper. In particular, it is an instance of Theorem 7 in case of $n_1 \geq n_2 \geq n_e$; and an instance of Theorem 9 in case of $n_e \leq n_2 \leq 2n_e$. Its individual secrecy capacity is shown in Fig. 2, and can be obtained by taking $U = Y_2 = D^{n_1-n_2}X$ (it is assumed that $n_2 \leq n_1$) and $V = X$ in the superposition coding as described in Theorem 5.

C. Marton's coding approach

In the previous subsection, the superposition coding approach is shown to be optimal for some special cases if the receivers and the eavesdropper fulfill a certain degradation/less noisiness order.

Here, we consider the general case where there may not be degradation/less noisiness order between the legitimate receivers, and devise a coding scheme by utilizing Marton's coding, attempting to send extra secret information to both legitimate receivers. In particular, the common message extended version of Marton's coding approach allows for a transmission of a cloud center to *both* receivers. In addition to this cloud center, two separate codewords can be formed via the Marton's coding. We have the following result.

Theorem 10. *For the DM-BC with an external eavesdropper, an achievable individual secrecy rate region is given by the union of rate pairs $(R_1, R_2) \in \mathcal{R}_+^2$ with $R_1 = R_{1s} + R_{1k}$ and $R_2 = R_{2s} + R_{2k}$, where $(R_{1k}, R_{1s}, R_{2k}, R_{2s}) \in \mathcal{R}_+^4$, that satisfies*

$$\begin{aligned} R_{1s} &\leq I(V_1;Y_1|U) - I(V_1;Z|U) \\ R_{2s} &\leq I(V_2;Y_2|U) - I(V_2;Z|U) \\ R_k + R_{1s} &\leq I(U,V_1;Y_1) - I(V_1;Z|U) \\ R_k + R_{2s} &\leq I(U,V_2;Y_2) - I(V_2;Z|U) \end{aligned} \tag{24}$$

with

$$R_k = \max\left\{R_{1k} + R_{2k}, \max\{R_{1k}, R_{2k}\} + I(U;Z)\right\} \tag{25}$$

over all $p(u)p(v_1,v_2|u)p(x|v_1,v_2)$ *subject to* $I(V_1;V_2|U)+I(V_1,V_2;Z|U)\leq I(V_1;Z|U)+I(V_2;Z|U)$;

Or, equivalently in terms of (R_1,R_2),

$$\begin{aligned}
R_2 &\leq [I(V_2;Y_2|U)-I(V_2;Z|U)]^+ + I(U;Y_2)-I(U;Z)\\
R_2 &\leq \sum_{i=1}^{2}[I(V_i;Y_i|U)-I(V_i;Z|U)]^+ + I(U;Y_1)-I(U;Z)\\
R_1 &\leq [I(V_1;Y_1|U)-I(V_1;Z|U)]^+ + I(U;Y_1)-I(U;Z)\\
R_1 &\leq \sum_{i=1}^{2}[I(V_i;Y_i|U)-I(V_i;Z|U)]^+ + I(U;Y_2)-I(U;Z)\\
R_1+R_2 &\leq \sum_{i=1}^{2}[I(V_i;Y_i|U)-I(V_i;Z|U)]^+ + \min\{I(U;Y_1),I(U;Y_2)\}
\end{aligned} \tag{26}$$

over all $p(u)p(v_1,v_2|u)p(x|v_1,v_2)$ *subject to* $I(V_1;V_2|U)+I(V_1,V_2;Z|U)\leq I(V_1;Z|U)+I(V_2;Z|U)$.

Proof: See Appendix E. ■

The coding approach we develop here is built on the aforementioned primitive approach and superposition approach, but with the framework of Marton's coding. That is, we split M_i into $M_i=(M_{ik},M_{is})$, for $i=1,2$. In particular, (M_{1k},M_{2k}) are encoded into the cloud codeword U^n (as in the primitive approach), where individual secrecy is guaranteed by employing Carleial-Hellman's secrecy coding; moreover, additional information M_{1s},M_{2s} are carried by individual satellite codewords V_1^n,V_2^n, respectively, (as in the superposition approach for each legitimate receiver). Note that, the secrecy of M_{is} for $i=1,2$, is ensured by employing Wyner's secrecy coding. Finally, following the spirit of Marton's coding, (V_1^n,V_2^n) is chosen jointly, and corresponding codeword X^n is sent to the channel.

As reflected in the obtained region in (24), R_k (as defined in (25)) is contributed by applying Carleial-Hellman's secrecy coding in the cloud layer on (M_{1k},M_{2k}) to obtain their individual secrecy; the first two inequalities are contributed by employing Wyner's secrecy coding in the individual satellite layer to ensure the secrecy of the extra message M_{is} to each legitimate receiver i. The last two inequalities in (24) come from the fact that receiver i, $i=1,2$, uses indirect decoding to decode $m_i=(m_{ik},m_{is})$ and there is a rate loss of $I(V_i;Z|U)$ for the sake of the individual secrecy.

Remark: We report the following observations:

- Setting $V_1,V_2,X=U$, i.e., $R_{1s}=R_{2s}=0$, the region reduces to the one in (14) by the primitive approach.
- If we let $V_2=U$ and $X=V_1$, i.e., $R_{2s}=0$, the region reduces to the one in (16) by the superposition approach.

D. Joint secrecy rate region

Revising the secrecy proofs by fulfilling the joint secrecy constraints (5) (instead of the individual secrecy constraints (3) as considered in previous subsections), we obtain achievable joint secrecy rate region by utiliz-

ing the aforementioned coding approaches. We note that both the primitive approach and the superposition approach serve as underneath coding layers for the Marton's coding approach. Therefore, their resultant rate regions are also included as special cases of the region derived by the Marton's coding approach, which is given as follows.

Theorem 11. *(Achievable joint secrecy rate region via Marton's coding) For the DM-BC with an external eavesdropper, an achievable joint secrecy rate region obtained by Marton's coding is the union of the rate pairs* $(R_1, R_2) \in \mathcal{R}_+^2$ *satisfying*

$$\begin{aligned} R_1 &\leq [I(V_1;Y_1|U) - I(V_1;Z|U)]^+ + I(U;Y_1) - I(U;Z) \\ R_2 &\leq [I(V_2;Y_2|U) - I(V_2;Z|U)]^+ + I(U;Y_2) - I(U;Z) \\ R_1 + R_2 &\leq \sum_{i=1}^{2} [I(V_i;Y_i|U) - I(V_i;Z|U)]^+ + \min\{I(U;Y_1), I(U;Y_2)\} - I(U;Z) \end{aligned} \tag{27}$$

over any $p(u, v_1, v_2, x) = p(u)p(v_1, v_2|u)p(x|v_1, v_2)$ *subject to* $I(V_1, V_2; Z|U) \leq I(V_1; Z|U) + I(V_2; Z|U) - I(V_1; V_2|U)$.

Proof: See Appendix G. ■

Remark: We have the following observations:

- In case that Y_1 is less noisy than Y_2, one can take $U = V_2$, then the region (27) reduces to

$$\begin{aligned} R_2 &\leq I(U;Y_2) - I(U;Z) \\ R_1 + R_2 &\leq [I(V_1;Y_1|U) - I(V_1;Z|U)]^+ + I(U;Y_2) - I(U;Z). \end{aligned} \tag{28}$$

  As shown in [7], [30], (28) is the joint secrecy capacity region of the degraded broadcast channel. Interestingly, comparing (28) with (23), the only difference is that the term $[I(V_1;Y_1|U) - I(V_1;Z|U)]^+ + I(U;Y_2) - I(U;Z)$ upper bounds the sum rate $R_1 + R_2$ in (28) under the joint secrecy constraint, while it upper bounds R_1 in (23) under the individual secrecy constraint. This implies that in case of a comparable eavesdropper (i.e., $I(U;Z) \leq I(U;Y_2) \leq 2I(U;Z)$ holds for any $p(u, v, x)$), the strong receiver could gain in the transmission rate up to that of the weak receiver when a weaker (individual) secrecy constraint is imposed.
- Compare (27) with the individual secrecy achievable region in (26). There is a gain of $I(U;Z)$ bits on the sum transmission rate $R_1 + R_2$ as a trade for having a weaker notion of security.
- [10, Theorem 1] gives an achievable rate region of the BC with two receivers and one eavesdropper, where the transmitter wants to transmit a pair of public and confidential messages to each legitimate receiver. (No secrecy constraints on the public messages, but two confidential messages are required to fulfill the joint secrecy constraint at the eavesdropper.) Setting both rates for two public messages to

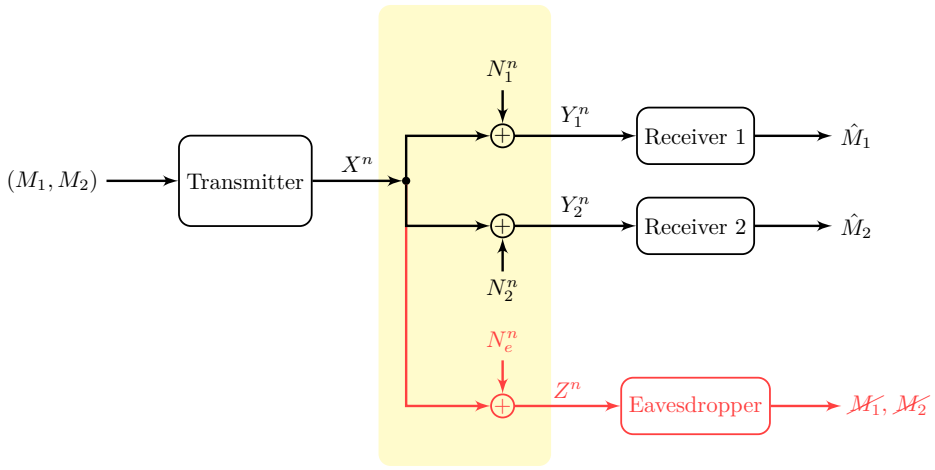


Fig. 3: Gaussian BC with an external eavesdropper.

be zero in [10, Theorem 1], one can obtain the following achievable joint secrecy rate region:

$$\begin{aligned} R_1 &\le [I(V_1;Y_1|U) - I(V_1;Z|U)]^+ + \min\{I(U;Y_1), I(U;Y_2)\} - I(U;Z) \\ R_2 &\le [I(V_2;Y_2|U) - I(V_2;Z|U)]^+ + \min\{I(U;Y_1), I(U;Y_2)\} - I(U;Z) \\ R_1 + R_2 &\le \sum_{i=1}^{2} I(V_i;Y_i|U) + \min\{I(U;Y_1), I(U;Y_2)\} - I(V_1;V_2|U) - I(U,V_1,V_2;Z) \end{aligned} \tag{29}$$

over any $p(u, v_1, v_2, x) = p(u)p(v_1, v_2|u)p(x|v_1, v_2)$ subject to $I(V_1, V_2; Z|U) \le I(V_1; Z|U) + I(V_2; Z|U) - I(V_1; V_2|U)$ and $I(U; Z) \le I(U; Y_i)$, $I(V_i; Z|U) \le I(V_i; Y_i|U)$ for $i = 1, 2$.

Comparing (29) with our joint secrecy rate region result in (27), we see that our upper bounds on R_1, R_2 are potentially greater while the upper bound on $R_1 + R_2$ is potentially smaller. The reason is caused by the fact that in our achievablility scheme, indirect decoding is applied at each legitimate receiver (note that joint unique decoding works the same here without any potential rate loss); while in [10], sequential decoding is employed at both legitimate receivers (i.e., decode U^n first, then V_i^n. This also results in an additional constraint on U, i.e., $I(U; Z) \le I(U; Y_i)$ for $i = 1, 2$). Besides, the difference on the sum rate bound is due to the fact that in our joint secrecy proof, V_1^n, V_2^n, are processed individually, whereas in [10, Theorem 1] (V_1^n, V_2^n) as jointly.

V. Gaussian BC with an external eavesdropper

The Gaussian BC with an external eavesdropper is shown in Fig. 3. Suppose X is the channel input with a power constraint P on it and the signals received by both receivers and the eavesdropper are given by

$$Y_1 = X + N_1;$$

$$Y_2 = X + N_2;$$

$$Z = X + N_e,$$

where N_1, N_2 and N_e are additive white Gaussian noise (AWGN) independent of X, where $N_1 \sim \mathcal{N}(0, \sigma_1^2)$, $N_2 \sim \mathcal{N}(0, \sigma_2^2)$ and $N_e \sim \mathcal{N}(0, \sigma_e^2)$, respectively.

According to the noise level in the channels to both receivers and the eavesdropper, the overall channel can be regarded to be *stochastically* degraded. For simplicity, we only consider its corresponding *physically* degraded instances. The reason is that the same analysis can be easily extended to the stochastically degraded case. That is, the scenario: $\sigma_e^2 \geq \sigma_2^2 \geq \sigma_1^2$, as $X \to Y_1 \to Y_2 \to Z$ forms a Markov chain, is of our interest.

In the previous section, single-letter expressions for the achievable individual secrecy rate regions and upper bounds have been proposed for the DM-BC, which involve auxiliary variable U and V. Applying the standard discretization procedure [19], one can extend these results to the Gaussian case. However, it is in general not clear what would be the optimal choice of (U, V). In this section, we are going to derive *computable* inner and outer bounds on the individual secrecy capacity region of the Gaussian BC with an external eavesdropper. Interestingly, we show that our inner bound (by employing the superposition coding) approaches the individual secrecy capacity region within a constant gap (i.e., 0.5 bits).

A. An outer bound

Theorem 12. *An outer bound to the individual secrecy capacity region for the Gaussian BC with an external eavesdropper (where $X \to Y_1 \to Y_2 \to Z$ forms a Markov chain) is given by the union of the rate pairs $(R_1, R_2) \in \mathcal{R}_+^2$ satisfying*

$$R_1 \leq C\left(\frac{\alpha(1-\gamma)P}{\gamma\alpha P + \sigma_1^2}\right) - C\left(\frac{\alpha(1-\gamma)P}{\gamma\alpha P + \sigma_e^2}\right) + \min\left\{R_2, C\left(\frac{(1-\gamma\alpha)P}{\gamma\alpha P + \sigma_e^2}\right)\right\} \tag{30}$$

$$R_2 \leq C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_2^2}\right) - C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_e^2}\right), \tag{31}$$

where $\alpha, \gamma \in [0, 1]$.

Proof: First let us consider R_2.

$$\begin{aligned} nR_2 = H(M_2) &\overset{(a)}{\leq} I(M_2; Y_2^n) + n\lambda_2(\epsilon_n) \\ &\overset{(b)}{\leq} I(M_2; Y_2^n) - I(M_2; Z^n) + n\lambda_2(\epsilon_n, \tau_n) \\ &= \underbrace{h(Y_2^n) - h(Z^n)}_{nR_2^1} - \underbrace{(h(Y_2^n|M_2) - h(Z^n|M_2))}_{nR_2^2} + n\lambda_2(\epsilon_n, \tau_n), \end{aligned}$$

where (a) is due to the reliability constraint (2), Fano's inequality and by taking $\lambda_2(\epsilon_n) = 1/n + \epsilon_n R_2$; (b) is due to the individual secrecy constraint (3) and by taking $\lambda_2(\epsilon_n, \tau_n) = \tau_n + \lambda_2(\epsilon_n)$.

Note that according to [31, Lemma 10 and equation (75)], nR_2^1 can be bounded by:

$$nR_2^1 = h(Y_2^n) - h(Z^n) \leq \frac{n}{2} \log \frac{P + \sigma_2^2}{P + \sigma_e^2}. \tag{32}$$

Further, due to the channel degradedness, we have for nR_2^2 :

$$nR_2^2 \geq h(Y_2^n|X^n) - h(Z^n|X^n) = \frac{n}{2}\log\frac{\sigma_2^2}{\sigma_e^2};$$
$$nR_2^2 \leq h(Y_2^n) - h(Z^n) \leq \frac{n}{2}\log\frac{P+\sigma_2^2}{P+\sigma_e^2}.$$

Hence, there exists an $\alpha \in [0,1]$ such that

$$nR_2^2 = h(Y_2^n|M_2) - h(Z^n|M_2) = \frac{n}{2}\log\frac{\alpha P+\sigma_2^2}{\alpha P+\sigma_e^2}. \tag{33}$$

Combining (32) and (33), we have

$$\begin{aligned} nR_2 &= nR_2^1 - nR_2^2 + n\lambda_2(\epsilon_n,\tau_n) \\ &\leq \frac{n}{2}\log\frac{P+\sigma_2^2}{P+\sigma_e^2} - \frac{n}{2}\log\frac{\alpha P+\sigma_2^2}{\alpha P+\sigma_e^2} + n\lambda_2(\epsilon_n,\tau_n) \\ &= \frac{n}{2}\log\frac{(P+\sigma_2^2)(\alpha P+\sigma_e^2)}{(\alpha P+\sigma_2^2)(P+\sigma_e^2)} + n\lambda_2(\epsilon_n,\tau_n). \end{aligned}$$

That is,

$$R_2 \leq C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_2^2}\right) - C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_e^2}\right) + \lambda_2(\epsilon_n,\tau_n). \tag{34}$$

Now we proceed to bound R_1.

$$\begin{aligned} nR_1 = H(M_1) = H(M_1|M_2) &\overset{(c)}{\leq} I(M_1;Y_1^n|M_2) + n\lambda_1(\epsilon_n) \\ &= I(M_1;Y_1^n|M_2) - I(M_1;Z^n|M_2) + I(M_1;Z^n|M_2) + n\lambda_1(\epsilon_n) \\ &= \underbrace{h(Y_1^n|M_2) - h(Z^n|M_2)}_{nR_1^1} - \underbrace{(h(Y_1^n|M_1,M_2) - h(Z^n|M_1,M_2))}_{nR_1^2} + \underbrace{I(M_1;Z^n|M_2)}_{nR_1^3} + n\lambda_1(\epsilon_n), \end{aligned} \tag{35}$$

where (c) is due to the reliability constraint (2), Fano's inequality and by taking $\lambda_1(\epsilon_n) = 1/n + \epsilon_n R_1$.

Applying Costa's entropy power inequality (EPI) [32, Theorem 1] and using (33), we obtain

$$nR_1^1 = h(Y_1^n|M_2) - h(Z^n|M_2) \leq \frac{n}{2}\log\frac{\alpha P+\sigma_1^2}{\alpha P+\sigma_e^2}. \tag{36}$$

(A more detailed proof of (36) is given in Appendix H.)

For nR_1^2, due to the channel degradedness, we have

$$nR_1^2 \geq h(Y_1^n|X^n) - h(Z^n|X^n) = \frac{n}{2}\log\frac{\sigma_1^2}{\sigma_e^2};$$
$$nR_1^2 \leq h(Y_1^n|M_2) - h(Z^n|M_2) \leq \frac{n}{2}\log\frac{\alpha P+\sigma_1^2}{\alpha P+\sigma_e^2}.$$

Hence, there exists a $\gamma \in [0,1]$ such that

$$\begin{aligned} nR_1^2 &= h(Y_1^n|M_1,M_2) - h(Z^n|M_1,M_2) \\ &= \frac{n}{2}\log\frac{\gamma\alpha P+\sigma_1^2}{\gamma\alpha P+\sigma_e^2}. \end{aligned} \tag{37}$$

Applying the entropy power inequality (EPI) [33] and using (37) for $h(Y_1^n|M_1,M_2)-h(Z^n|M_1,M_2)$, we can bound $h(Z^n|M_1,M_2)$ by

$$h(Z^n|M_1,M_2) \geq \frac{n}{2}\log 2\pi e(\gamma\alpha P+\sigma_e^2). \tag{38}$$

(A more detailed proof of (38) is given in Appendix I.)

For nR_1^3, we observe that

$$\begin{aligned} nR_1^3 &= I(M_1;Z^n|M_2) = I(M_1,M_2;Z^n) - I(M_2;Z^n) \\ &= I(M_2;Z^n|M_1) + I(M_1;Z^n) - I(M_2;Z^n) \\ &\overset{(d)}{\leq} nR_2 + n\tau_n, \end{aligned}$$

where (d) is due to the individual secrecy constraint (3).

Moreover, we can bound nR_1^3 as follows

$$\begin{aligned} nR_1^3 &= I(M_1;Z^n|M_2) = h(Z^n|M_2) - h(Z^n|M_1,M_2) \\ &\leq h(Z^n) - h(Z^n|M_1,M_2) \\ &\leq \frac{n}{2}\log\frac{P+\sigma_e^2}{\gamma\alpha P+\sigma_e^2}. \end{aligned}$$

Therefore, we have so far

$$\begin{aligned} nR_1 &= nR_1^1 - nR_1^2 + nR_1^3 + n\lambda_1(\epsilon_n) \\ &\leq \frac{n}{2}\log\frac{\alpha P+\sigma_1^2}{\alpha P+\sigma_e^2} - \frac{n}{2}\log\frac{\gamma\alpha P+\sigma_1^2}{\gamma\alpha P+\sigma_e^2} + \min\left\{nR_2, \frac{n}{2}\log\frac{P+\sigma_e^2}{\gamma\alpha P+\sigma_e^2}\right\} + n\lambda_1(\tau_n,\epsilon_n) \\ &= \frac{n}{2}\log\frac{\alpha P+\sigma_1^2}{\gamma\alpha P+\sigma_1^2} - \frac{n}{2}\log\frac{\alpha P+\sigma_e^2}{\gamma\alpha P+\sigma_e^2} + \min\left\{nR_2, \frac{n}{2}\log\frac{P+\sigma_e^2}{\gamma\alpha P+\sigma_e^2}\right\} + n\lambda_1(\tau_n,\epsilon_n), \end{aligned}$$

where $\lambda_1(\tau_n,\epsilon_n)=\tau_n+\lambda_1(\epsilon_n)$. That is,

$$R_1 \leq C\left(\frac{\alpha(1-\gamma)P}{\gamma\alpha P+\sigma_1^2}\right) - C\left(\frac{\alpha(1-\gamma)P}{\gamma\alpha P+\sigma_e^2}\right) + \min\left\{R_2, C\left(\frac{(1-\gamma\alpha)P}{\gamma\alpha P+\sigma_e^2}\right)\right\} + \lambda_1(\tau_n,\epsilon_n). \tag{39}$$

Letting $n\to\infty, \tau_n, \epsilon_n \to 0$, we have $\lambda_1(\tau_n,\epsilon_n), \lambda_2(\tau_n,\epsilon_n)\to 0$; and (39), (34) reduce to (30), (31), respectively. This completes our proof. ■

By Theorem 12, we easily obtain a looser outer bound as described in the following corollary.

Corollary 13. *An outer bound to the individual secrecy capacity region for the Gaussian BC with an external eavesdropper (where $X\to Y_1\to Y_2\to Z$ forms a Markov chain) is given by the union of the rate pairs $(R_1,R_2)\in\mathcal{R}_+^2$ satisfying*

$$\begin{aligned} R_1 &\leq C\left(\frac{\alpha P}{\sigma_1^2}\right) - C\left(\frac{\alpha P}{\sigma_e^2}\right) + C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_2^2}\right) - C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_e^2}\right) \\ R_2 &\leq C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_2^2}\right) - C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_e^2}\right) \\ R_1+R_2 &\leq C\left(\frac{\alpha P}{\sigma_1^2}\right) + C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_2^2}\right), \end{aligned} \tag{40}$$

where $\alpha \in [0,1]$.

Proof: See Appendix J ■

B. An inner bound

Theorem 14. *An inner bound of the individual secrecy capacity region for the Gaussian BC with an external eavesdropper (where* $X \to Y_1 \to Y_2 \to Z$ *forms a Markov chain) is given by the union of the rate pairs* $(R_1, R_2) \in \mathcal{R}_+^2$ *satisfying*

$$\begin{aligned} R_1 \leq & C\left(\frac{\alpha P}{\sigma_1^2}\right) - C\left(\frac{\alpha P}{\sigma_e^2}\right) + C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_2^2}\right) - C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_e^2}\right) \\ R_2 \leq & C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_2^2}\right) - C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_e^2}\right) \\ R_1 + R_2 \leq & C\left(\frac{\alpha P}{\sigma_1^2}\right) - C\left(\frac{\alpha P}{\sigma_e^2}\right) + C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_2^2}\right), \end{aligned} \tag{41}$$

where $\alpha \in [0,1]$.

Proof: The region is obtained from Theorem 5 by using jointly Gaussian (U, V) with $U \sim \mathcal{N}(0, (1-\alpha)P)$, $V \sim \mathcal{N}(0, \alpha P)$, $X = U + V$, where U and V are independent and $\alpha \in [0,1]$. ■

C. Individual secrecy capacity region

Theorem 15. *As* $\sigma_e^2 \geq \sigma_2^2 \geq \sigma_1^2$ *and* $P \geq \sigma_e^2(\sigma_e^2 - 2\sigma_2^2)/\sigma_2^2$, *the individual secrecy capacity region for the Gaussian BC with an external eavesdropper is given by the union of the rate pairs* $(R_1, R_2) \in \mathcal{R}_+^2$ *satisfying*

$$\begin{aligned} R_1 \leq & C\left(\frac{\alpha P}{\sigma_1^2}\right) - C\left(\frac{\alpha P}{\sigma_e^2}\right) + C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_2^2}\right) - C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_e^2}\right) \\ R_2 \leq & C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_2^2}\right) - C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_e^2}\right), \end{aligned}$$

where $\alpha \in [0,1]$. *In particular when* $\sigma_1^2 \leq \sigma_2^2 \leq \sigma_e^2 \leq 2\sigma_2^2$, *the above region serves as the individual secrecy capacity region for all power levels.*

Proof: Consider the inner bound (41). We see that when $R_2 \leq C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_e^2}\right)$ holds, then the sum rate bound in (41) becomes redundant. In the case that it holds for any $\alpha \in [0,1]$, the inner bound (41) coincides with the outer bound (40). This happens if $\max R_2 \leq C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_e^2}\right)$, i.e.,

$$C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_2^2}\right) - C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_e^2}\right) \leq C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_e^2}\right). \tag{42}$$

Under the stated conditions $\sigma_e^2 \geq \sigma_2^2 \geq \sigma_1^2$ and $P \geq \sigma_e^2(\sigma_e^2 - 2\sigma_2^2)/\sigma_2^2$, the inequality above, (42), holds if and only if $\alpha \geq \frac{(\sigma_e^2 - \sigma_2^2)^2}{P(P+\sigma_2^2)} - \frac{\sigma_2^2}{P} =$. (A detailed calculation is given in Appendix L.) As $\alpha \geq 0$, (42) holds regardless of the value of α, if $\frac{(\sigma_e^2 - \sigma_2^2)^2}{P(P+\sigma_2^2)} - \frac{\sigma_2^2}{P} \leq 0$ which hold as $P \geq \sigma_e^2(\sigma_e^2 - 2\sigma_2^2)/\sigma_2^2$. Finally, we note that this last condition always holds if $\sigma_2^2 \leq \sigma_e^2 \leq 2\sigma_2^2$ as $P \geq 0$. ■

Remark: Theorem 15 establishes the individual secrecy capacity region for all power levels for the comparable eavesdropper channel scenario (i.e., having $\sigma_2^2 \leq \sigma_e^2 \leq 2\sigma_2^2$). This is the counterpart of Theorem 9

for the Gaussian scenario: We have $I(U;Y_2) \leq 2I(U;Z)$ for any $U \sim \mathcal{N}(0,(1-\alpha)P)$, $\alpha \in [0,1]$. In this case, the superposition coding is optimal to achieve the individual secrecy capacity region.

For the scenarios where the condition in Theorem 15 does not hold, i.e., when $P < \sigma_e^2(\sigma_e^2 - 2\sigma_2^2)/\sigma_2^2$, we note that the same achievable scheme achieves the capacity region in an approximate manner (within half a bit) as established in the following result.

Theorem 16. *The achievable individual secrecy rate region as described in Theorem 14, i.e., the set of* $(R_1,R_2) \in \mathcal{R}_+^2$ *satisfying* (41)*, approaches the individual secrecy capacity region of the Gaussian BC within 0.5 bits.*

Proof: See Appendix K ∎

D. Numerical results with different secrecy constraints

In this subsection, we provide the capacity region results for the Gaussian BC without secrecy constraint and under the joint secrecy constraint, and make comparisons with our results on the individual secrecy capacity region that are derived in the previous subsection.

Theorem 17. *[19, Theorem 5.3] The capacity region of the Gaussian BC without secrecy constraint is given by the union of the rate pairs* $(R_1,R_2) \in \mathcal{R}_+^2$ *satisfying*

$$\begin{aligned} R_1 &\leq C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_2^2}\right) \\ R_2 &\leq C\left(\frac{\alpha P}{\sigma_1^2}\right), \end{aligned} \tag{43}$$

where $\alpha \in [0,1]$.

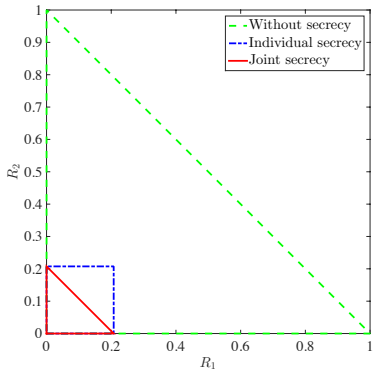
Theorem 18. *[20, Theorem 5] The joint secrecy capacity region of the Gaussian BC with an external eavesdropper is given by the union of the rate pairs* $(R_1,R_2) \in \mathcal{R}_+^2$ *satisfying*

$$\begin{aligned} R_1 &\leq C\left(\frac{\alpha P}{\sigma_1^2}\right) - C\left(\frac{\alpha P}{\sigma_e^2}\right) \\ R_2 &\leq C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_1^2}\right) - C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_e^2}\right), \end{aligned} \tag{44}$$

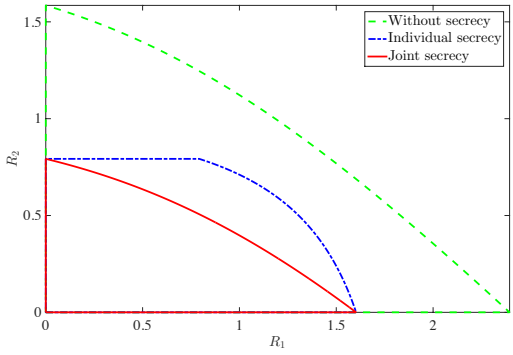
where $\alpha \in [0,1]$.

For the Gaussian BC, its capacity regions (or bounds) under different secrecy constraints are depicted in Fig. 4 (non-trivial case of $\sigma_1^2 \leq \sigma_2^2 \leq \sigma_e^2$ is assumed as detailed earlier). The capacity region without secrecy constraint is enclosed by (green) dashed lines; the joint secrecy capacity region is enclosed by (red) solid lines; whilst the individual secrecy capacity region or its inner bound are enclosed by (blue) dash-dotted lines, and the outer bound by (magenta) dotted lines. We observe the followings.

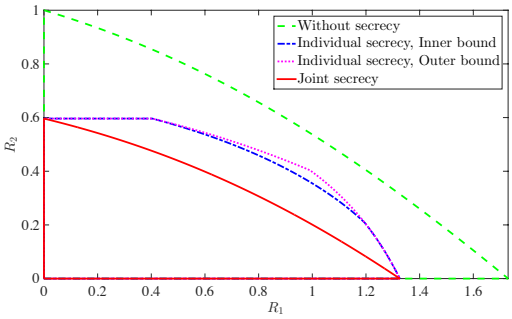
In Fig. 4a and Fig. 4b, we plot capacity regions under different secrecy constraints for some special cases that satisfy the condition requested in Theorem 15, in which, we have for any joint secrecy achievable



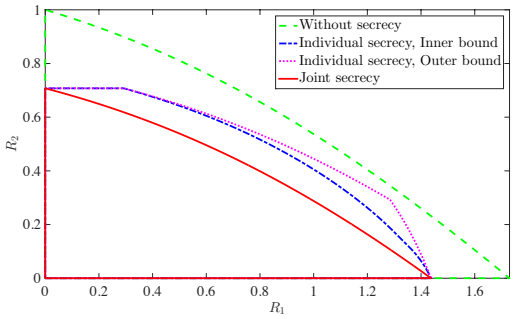
(a) $P = 1, \sigma_1^2 = \sigma_2^2 = 1/3, \sigma_e^2 = 1/2$



(b) $P = 1, \sigma_1^2 = 3/80, \sigma_2^2 = 1/8, \sigma_e^2 = 1/2$



(c) $P = 1, \sigma_1^2 = 1/10, \sigma_2^2 = 1/3, \sigma_e^2 = 4/3$



(d) $P = 1, \sigma_1^2 = 1/10, \sigma_2^2 = 1/3, \sigma_e^2 = 2$

Fig. 4: Capacity regions of Gaussian BC, where the parameters are chosen such that the following inequalities are satisfied, in (a)-(b): $P \geq \sigma_e^2(\sigma_e^2 - 2\sigma_2^2)/\sigma_2^2$, further in (a): $\sigma_1^2 = \sigma_2^2$ and (b): $\sigma_1^2 < \sigma_2^2$; in (c)-(d): $P < \sigma_e^2(\sigma_e^2 - 2\sigma_2^2)/\sigma_2^2$, further in (c): $2\sigma_2^2 \leq \sigma_e^2 \leq P + 2\sigma_2^2$ and in (d): $\sigma_e^2 \geq P + 2\sigma_2^2$, respectively.

(R_1, R_2), that $(R_1 + R_2, R_2)$ is achievable with individual secrecy. More specifically, Fig. 4a depicts a special case where both legitimate receivers experience the same noise level. In this case, both the capacity regions without secrecy constraint and under joint secrecy constraint, are right angled isosceles triangles; while the capacity region under the individual secrecy constraint is a square, area of which doubles that of the joint secrecy case. Fig. 4b depicts a more general case where both legitimate receivers experience different noise levels. The maximum marginal transmission rates (say R_1^*, R_2^*, respectively) to both receivers are the same under either joint or individual secrecy constraints, which are strictly smaller than the ones for the scenario without any secrecy constraints. However, a distinct behavior for the individual secrecy capacity region is that, if the weak receiver operates at its maximum transmission rate, then the strong receiver can be still active (unlike the scenarios without secrecy constraint and under joint secrecy constraint). This

can be visualized by the top-left part of the blue dash-dotted curve, as a straight line. Especially, for this special case as depicted in Fig. 4b, we have (R_2^*, R_2^*) pair as individually secret. We note that, form Theorem 15, superposition coding is optimal and $I(U;Y_2) - I(U;Z) \leq I(U;Z)$ holds for any $U \sim \mathcal{N}(0,(1-\alpha)P)$, $\alpha \in [0,1]$. As receiver 2 operates at rate $R_2 \leq R_U$ with $R_U = I(U;Y_2) - I(U;Z)$, the information (say m_{1k}) up to R_U could be carried to receiver 1 via the cloud codeword U while maintaining the individual secrecy of m_2 and m_{1k}. Additional secret information to receiver 1 will be conveyed by the satellite codeword V, similar to the joint secrecy scenario.

In Fig. 4c and Fig. 4d, the parameters are chosen such that $P < \sigma_e^2(\sigma_e^2 - 2\sigma_2^2)/\sigma_2^2$, which does not satisfy the condition given in Theorem 15. Therefore, we use the inner bound (as given in Theorem 14) and the outer bound (as given in Corollary 13). More specifically, Fig. 4c depicts a case where $2\sigma_2^2 \leq \sigma_e^2 \leq P + 2\sigma_2^2$ (i.e., satisfying (114)). In this case, there exists an $\alpha_0 = \frac{(\sigma_e^2-\sigma_2^2)^2}{P(P+\sigma_2^2)} - \frac{\sigma_2^2}{P}$, such that a gap between the inner and outer bound occurs as $0 < \alpha \leq \alpha_0$. For the chosen parameter set, we have $\alpha_0 = 5/12$. That is, the inner bound is tight for $\alpha = 0$ and $\alpha \in [5/12, 1]$, which corresponds to the region where $R_2 = R_2^*$ (here $R_2^* = 0.7075$) and $R_2 \in [0, 0.2075]$, respectively. Fig. 4d depicts a case where $\sigma_e^2 \geq P + 2\sigma_2^2$ (i.e., satisfying (113)). In this case, the inner and outer bound coincide at $\alpha = 0$ but not for $0 < \alpha < 1$. This indicates that the top-left part of the (blue) dash-dotted curve, as a straight line, is tight for the individual secrecy. Differently from the scenarios in Fig. 4a and Fig. 4b, we notice that in Fig. 4c and Fig. 4d, (R_2^*, R_2^*) pair is *not* individually secret. The underlying reason is that $I(U;Y_2) - I(U;Z) \leq I(U;Z)$ does not hold for any $U \sim \mathcal{N}(0,(1-\alpha)P)$, $\alpha \in [0,1]$ in this case. In particular, in Fig. 4d, as $\alpha = 0$ (i.e., all the power is assigned to the U codeword), we have $R_2^* = I(U;Y_2) - I(U;Z) = 0.7075$ and $I(U;Z) = 0.2925$. As receiver 2 operates m_2 at rate $R_2^* = 0.7075$, the maximal information m_1 that could be carried to receiver 1 via the codeword U will be bounded by $I(U;Z) = 0.2925$ (according to (41) and (40)) while maintaining the individual secrecy of m_2 and m_1.

VI. Conclusion

In this paper, we studied the problem of secure communication over degraded broadcast channel under the individual secrecy constraint. Compared to the joint secrecy constraint, this relaxed setting allows for higher secure communication rates at the expense of having a weaker notion of security. As a general result, we derived several achievable rate regions and characterized the individual secrecy capacity region for some special cases. In addition, we also investigated the linear deterministic model and the Gaussian model. For the linear deterministic model, the capacity regions are fully characterized for the cases without secrecy constraint, under joint and individual secrecy constraint; while for the Gaussian model, a constant gap (i.e., 0.5 bits within the individual secrecy capacity region) result is obtained. Comparisons are made among the capacity regions for both models with different secrecy constraints (under no/individual/joint secrecy cases).

Appendix A
Proof of Theorem 1

The converse can be shown as follows: The first two inequalities for R_1, R_2, respectively, follow from the classical results of wiretap channel by simply ignoring the other legitimate receiver. And, the last inequality follows directly from the upper bound on the sum rate for the relaxed case of without any secrecy constraints.

The achievability can be shown by considering different scenarios, which is classified according to the relation between the channel gains n_1, n_2, n_e, and the relation between the rates R_1, R_2. Under the assumption that $n_1 \geq n_2$, for both cases of $q = n_1 \geq n_e \geq n_2$ and $n_e \geq n_1 \geq n_2$, the individual secrecy capacity region reduces to the one for the wiretap channel [13], [14] and the achievability follows therein. Here we only need to consider the rest case $q = n_1 \geq n_2 \geq n_e$. The detailed achievability proof is given as follows.

- If $R_2 \leq n_e$, we have two scenarios:

  1) $R_1 \leq R_2$. For this scenario, (11) reduces to the following:

  $$R_1 \leq R_2 \leq \min\{n_2 - n_e, n_e\}.$$

  For its achievability, given m_1, m_2 with $m_1 = [m_1(1), \cdots, m_1(R_1)]$ and $m_2 = [m_2(1), \cdots, m_2(R_2)]$, we send $X = [x(1), x(2), \cdots, x(n_1)]^T$ such that

  $$x(k) = \begin{cases} m_1(k) \oplus m_2(k) & 1 \leq k \leq R_1 \\ r(k) & R_1 < k \leq n_e \\ m_2(k - n_e) & n_e < k \leq n_e + R_2 \\ r(k) & n_e + R_2 < k \leq n_1 \end{cases}$$

  where $r(k)$ is randomly chosen from $\{0, 1\}$. The construction of X is illustrated in Fig. 5.

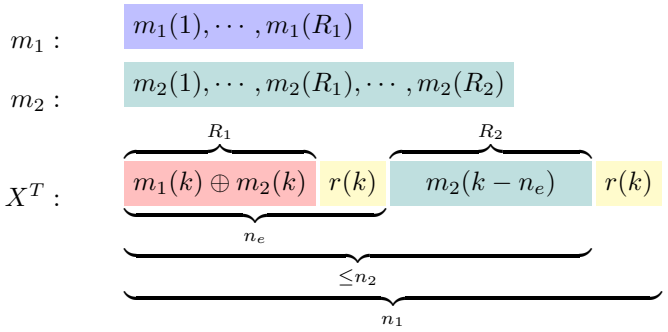


Fig. 5: Codeword X for a) $R_1 \leq R_2 \leq n_e$.

  2) $R_1 \geq R_2$. For this scenario, (11) reduces to the following:

  $$R_2 \leq R_1 \leq n_1 - n_e; \quad R_2 \leq \min\{n_e, n_2 - n_e\}.$$

For its achievability, given m_1, m_2 with $m_1 = [m_1(1), \cdots, m_1(R_1)]$ and $m_2 = [m_2(1), \cdots, m_2(R_2)]$, we send $X = [x(1), x(2), \cdots, x(n_1)]^T$ such that

$$x(k) = \begin{cases} m_1(k) \oplus m_2(k) & 1 \le k \le R_2 \\ r(k) & R_2 < k \le n_e \\ m_2(k - n_e) & n_e < k \le n_e + R_2 \\ m_1(k - n_e - R_2) & n_e + R_2 < k \le n_e + R_1 \\ r(k) & n_e + R_1 < k \le n_1 \end{cases}$$

where $r(k)$ is randomly chosen from $\{0, 1\}$. The construction of X is illustrated in Fig. 6.

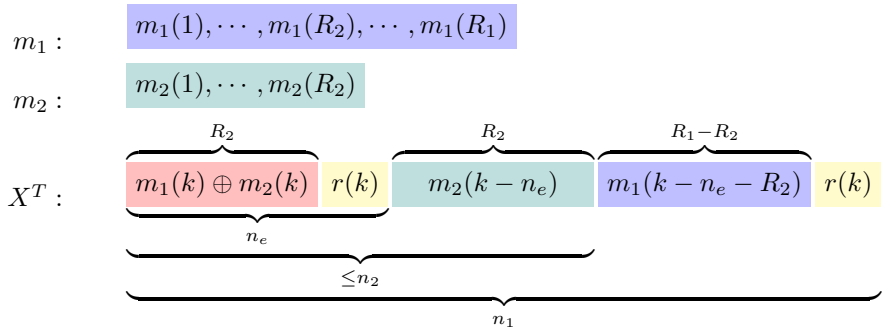


Fig. 6: Codeword X for b) $R_2 \le n_e$ and $R_2 \le R_1$.

- If $R_2 \ge n_e$, we also have two scenarios:

  1) $R_1 \le n_e$. For this scenario, (11) reduces to the following:

  $$R_1 \le n_e \le R_2 \le n_2 - n_e.$$

  Note that this scenario is possible only when $n_2 \ge 2n_e$. For its achievability, given m_1, m_2 with $m_1 = [m_1(1), \cdots, m_1(R_1)]$ and $m_2 = [m_2(1), \cdots, m_2(R_2)]$, we send $X = [x(1), x(2), \cdots, x(n_1)]^T$ such that

  $$x(k) = \begin{cases} m_1(k) \oplus m_2(k) & 1 \le k \le R_1 \\ r(k) & R_1 < k \le n_e \\ m_2(k - n_e) & n_e + 1 \le k \le n_e + R_2 \\ r(k) & n_e + R_2 < k \le n_1 \end{cases}$$

  where $r(k)$ is randomly chosen from $\{0, 1\}$. The construction of X is illustrated in Fig. 7.

  2) $R_1 \ge n_e$. For this scenario, (11) reduces to the following:

  $$n_e \le R_1 \le n_1 - n_e; \quad n_e \le R_2 \le n_2 - n_e.$$

  For its achievability, given m_1, m_2 with $m_1 = [m_1(1), \cdots, m_1(R_1)]$ and $m_2 = [m_2(1), \cdots, m_2(R_2)]$,

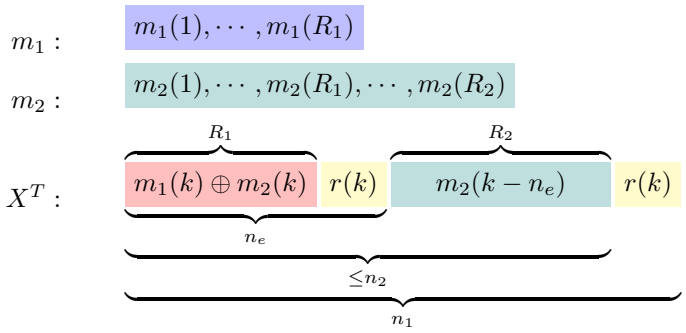


Fig. 7: Codeword X for c) $R_1 \leq n_e \leq R_2$.

we send $X = [x(1), x(2), \cdots, x(n_1)]^T$ such that

$$x(k) = \begin{cases} m_1(k) \oplus m_2(k) & 1 \leq k \leq n_e \\ m_2(k - n_e) & n_e < k \leq n_e + R_2 \\ m_1(k - R_2) & n_e + R_2 < k \leq R_1 + R_2 \\ r(k) & R_1 + R_2 < k \leq n_1 \end{cases}$$

where $r(k)$ is randomly chosen from $\{0, 1\}$. The construction of X is illustrated in Fig. 8.

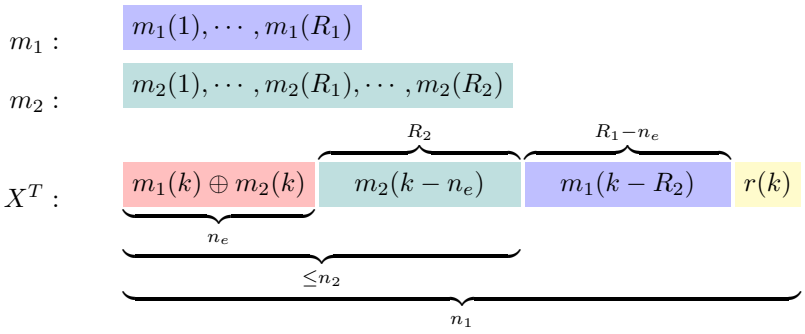


Fig. 8: Codeword X for d) $R_1 \geq n_e$ and $R_2 \geq n_e$.

Note that in all scenarios, receiver 1 gets the first n_1 bits of X; receiver 2 gets the first n_2 bits of X; while the eavesdropper gets the first n_e bits of X. Receiver 2 can obtain the desired message m_2; and receiver 1 obtains the message m_2 first and then could decode its desired message m_1 with the help of m_2; whilst the eavesdropper gets only $m_1(k) \oplus m_2(k)$ for $1 \leq k \leq \min\{n_e, R_1, R_2\}$ and some other random bits, which gives no information on m_1, m_2 individually.

Appendix B
Proof of Theorem 4

In the following, we provide the detailed achievability proof for a given $p(u, x)$.

Codebook generation: Fix $p(u)$. Randomly generate $2^{n(R_1+R_2+R_r)}$ i.i.d sequences $u^n(m_1, m_2, m_r)$, with $(m_1, m_2, m_r) \in [1 : 2^{nR_1}] \times [1 : 2^{nR_2}] \times [1 : 2^{nR_r}]$, according to $p(u)$.

Encoding: To send messages (m_1, m_2), randomly choose $m_r \in [1 : 2^{nR_r}]$ and find $u^n(m_1, m_2, m_r)$. Given $u^n(m_1, m_2, m_r)$, generate x^n according to $p(x|u)$, and transmit it to the channel. The choice of u^n is illustrated in Fig. 9.

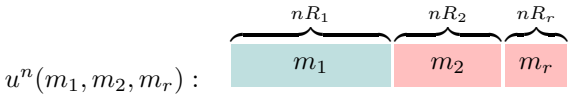


Fig. 9: Encoding

Decoding: Receiver 2, upon receiving y_2^n, finds $u^n(\hat{m}_1, \hat{m}_2, \hat{m}_r)$ such that $(u^n(\hat{m}_1, \hat{m}_2, \hat{m}_r), y_2^n)$ is jointly typical. Receiver 1, upon receiving y_1^n, finds $u^n(\tilde{m}_1, \tilde{m}_2, \tilde{m}_r)$ such that $(u^n(\tilde{m}_1, \tilde{m}_2, \tilde{m}_r), y_1^n)$ is jointly typical.

Analysis of the error probability of decoding: Assume that $(M_1, M_2) = (m_1, m_2)$ is sent.

First we consider $P_{e,2}$ at receiver 2. A decoding error happens iff one or both of the following events occur:

$$\begin{aligned}\mathcal{E}_{21} =&\{(u^n(m_1, m_2, m_r), y_2^n) \notin \mathcal{T}_\epsilon^{(n)}\},\\ \mathcal{E}_{22} =&\{(u^n(\hat{m}_1, \hat{m}_2, \hat{m}_r), y_2^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \hat{m}_2 \neq m_2\}.\end{aligned}$$

Thus, $P_{e,2}$ can be upper bounded as

$$P_{e,2} \leq \Pr(\mathcal{E}_{21}) + \Pr(\mathcal{E}_{22}).$$

By the LLN, $\Pr(\mathcal{E}_{21})$ tends to zero as $n \to \infty$. For $\Pr(\mathcal{E}_{22})$, since $u^n(\hat{m}_1, \hat{m}_2, \hat{m}_r)$ is independent of $(u^n(m_1, m_2, m_r), y_2^n)$ for $\hat{m}_2 \neq m_2$, by the packing lemma [19], $\Pr(\mathcal{E}_{22})$ tends to zero as $n \to \infty$ if

$$R_1 + R_2 + R_r \leq I(U; Y_2) - \delta_n(\epsilon_n). \tag{45}$$

Similarly, at receiver 1, the average probability of decoding error $P_{e,2}$, can be made arbitrarily small as $n \to \infty$ if

$$R_1 + R_2 + R_r \leq I(U; Y_1) - \delta_n(\epsilon_n). \tag{46}$$

Analysis of individual secrecy: For the individual secrecy (3), i.e., $R_{L,i} \leq \tau_n$, for $i = 1, 2$, it is equivalent to show that $H(M_i|Z^n) \geq H(M_i) - n\tau_n = nR_i - n\tau_n$. First we consider $H(M_2|Z^n)$.

$$\begin{aligned}H(M_2|Z^n) =&H(M_2, Z^n) - H(Z^n)\\ =&H(U^n, M_2, Z^n) - H(U^n|M_2, Z^n) - H(Z^n)\\ =&H(U^n) + H(Z^n|U^n) - H(U^n|M_2, Z^n) - H(Z^n)\\ \overset{(a)}{=}&n[R_1 + R_2 + R_r] + nH(Z|U) - H(U^n|M_2, Z^n) - H(Z^n)\\ \overset{(b)}{\geq}&n[R_1 + R_2 + R_r] - nI(U; Z) - H(U^n|M_2, Z^n)\end{aligned}$$

$$\begin{aligned}
&\overset{(c)}{\geq} n[R_1+R_2+R_r] - nI(U;Z) - n[R_1+R_r-I(U;Z)] - n\tau_n \\
&= nR_2 - n\tau_n \\
&= H(M_2) - n\tau_n,
\end{aligned}$$

where (a) follows from the codebook construction that $H(U^n) = n[R_1+R_{2k}+R_r]$ and the discrete memoryless of the channel; (b) is due to the fact that $H(Z^n) = \sum_{i=1}^{n} H(Z_i|Z^{i-1}) \leq \sum_{i=1}^{n} H(Z_i) = nH(Z)$; and (c) follows from [9, Lemma 1] that $H(U^n|M_2, Z^n) \leq n[R_1 + R_r - I(U;Z)] + n\tau_n$ if taking

$$R_1 + R_r \geq I(U;Z) + \delta_n(\tau_n). \tag{47}$$

A similar proof can be applied to show that $H(M_1|Z^n) \geq H(M_1) - n\tau_n$ if taking

$$R_2 + R_r \geq I(U;Z) + \delta_n(\tau_n). \tag{48}$$

Achievable individual secrecy rate region: The resulting region has the following constraints: the non-negativity for rates, i.e., $R_1, R_2, R_r \geq 0$, the conditions for a reliable communication, i.e., (45), (46), and the conditions for individual secrecy, i.e., (47), (48). Eliminating R_r here by applying Fourier-Motzkin procedure [19], we get the desired rate region as given in (14).

Appendix C
Proof of Theorem 5

For a given input probability distribution $p(u,v,x)$, let $I_1 = I(V;Y_1|U) - I(V;Z|U)$. If $I_1 \leq 0$, the claimed region reduces to (14), which is achievable by taking the primitive approach as described in Section IV-A, or more specifically, by employing Carleial-Hellman's secrecy coding. In the following, we provide the detailed achievability proof for the remaining case, i.e., if $I_1 > 0$ for a given $p(u,v,x)$.

Rate splitting: As illustrated in Fig. 10, we split M_1 into (M_{1k}, M_{1s}). In particular, M_{1k}, M_{1s} are of entropy nR_{1k} and nR_{1s}, respectively; and M_2 is of entropy nR_2. That is,

$$R_1 = R_{1k} + R_{1s}. \tag{49}$$

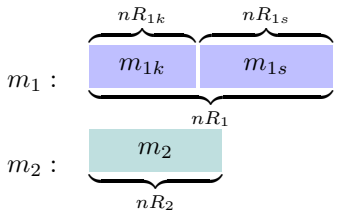


Fig. 10: Rate splitting

Codebook generation: Fix $p(u), p(v|u)$. First, randomly generate $2^{n(R_2+R_{1k}+R_r)}$ i.i.d. sequences $u^n(m_2, m_{1k}, m_r)$, with $(m_2, m_{1k}, m_r) \in [1 : 2^{nR_2}] \times [1 : 2^{nR_{1k}}] \times [1 : 2^{nR_r}]$, according to $p(u)$. Secondly, for each

$u^n(m_2, m_{1k}, m_r)$, randomly generate i.i.d. sequences $v^n(m_2, m_{1k}, m_r, m_{1s}, m_{1r})$ with $(m_{1s}, m_{1r}) \in [1 : 2^{nR_{1s}}] \times [1 : 2^{nR_{1r}}]$, according to $p(v|u)$.

Encoding: To send messages (m_1, m_2) with $m_1 = (m_{1k}, m_{1s})$, randomly choose $m_r \in [1 : 2^{nR_r}]$ and find $u^n(m_2, m_{1k}, m_r)$. Given $u^n(m_2, m_{1k}, m_r)$, randomly choose $m_{1r} \in [1 : 2^{nR_{1r}}]$, further find the corresponding $v^n(m_2, m_{1k}, m_r, m_{1s}, m_{1r})$. Generate x^n according to $p(x|v)$, and transmit it to the channel. The choice of u^n, v^n is illustrated in Fig. 11.

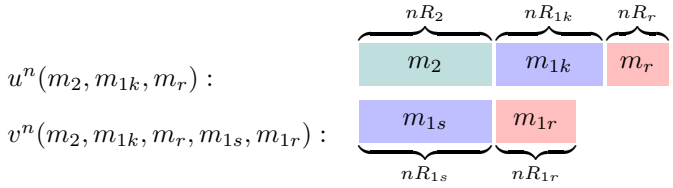


Fig. 11: Encoding

Decoding: Receiver 2, upon receiving y_2^n, finds $u^n(\hat{m}_2, \hat{m}_{1k}, \hat{m}_r)$ such that $(u^n(\hat{m}_2, \hat{m}_{1k}, \hat{m}_r), y_2^n)$ is jointly typical.

Receiver 1, upon receiving y_1^n, finds a unique tuple $(\tilde{m}_2, \tilde{m}_{1k}, \tilde{m}_r, \tilde{m}_{1s})$ $u^n(\tilde{m}_2, \tilde{m}_{1k}, \tilde{m}_r)$ such that $(u^n(\tilde{m}_2, \tilde{m}_{1k}, \tilde{m}_r), v^n(\tilde{m}_2, \tilde{m}_{1k}, \tilde{m}_r, \tilde{m}_{1s}, \tilde{m}_{1r}), y_1^n)$ is jointly typical for some $\tilde{m}_{1r}$. Finally, decode $\tilde{m}_1 = (\tilde{m}_{1k}, \tilde{m}_{1s})$.

Analysis of the error probability of decoding: Assume that $(M_1, M_2) = (m_1, m_2)$ with $m_1 = (m_{1k}, m_{1s})$ is sent.

First we consider $P_{e,2}$ at receiver 2. A decoding error happens iff one or both of the following events occur:

$$\mathcal{E}_{21} = \{(u^n(m_2, m_{1k}, m_r), y_2^n) \notin \mathcal{T}_\epsilon^{(n)}\},$$
$$\mathcal{E}_{22} = \{(u^n(\hat{m}_2, \hat{m}_{1k}, \hat{m}_r), y_2^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \hat{m}_2 \neq m_2\}.$$

Thus, $P_{e,2}$ can be upper bounded as

$$P_{e,2} \leq \Pr(\mathcal{E}_{21}) + \Pr(\mathcal{E}_{22}).$$

By the LLN, $\Pr(\mathcal{E}_{21})$ tends to zero as $n \to \infty$. For $\Pr(\mathcal{E}_{22})$, since $u^n(\hat{m}_2, \hat{m}_{1k}, \hat{m}_r)$ is independent of $(u^n(m_2, m_{1k}, m_r), y_2^n)$ for $\hat{m}_2 \neq m_2$, by the packing lemma [19], $\Pr(\mathcal{E}_{22})$ tends to zero as $n \to \infty$ if

$$R_2 + R_{1k} + R_r \leq I(U; Y_2) - \delta_n(\epsilon_n). \tag{50}$$

At receiver 1, the decoder makes an error iff one or more of the following events occur:

$$\mathcal{E}_{11} = \{(u^n(m_2, m_{1k}, m_r), v^n(m_2, m_{1k}, m_r, m_{1s}, m_{1r}), y_1^n) \notin \mathcal{T}_\epsilon^{(n)}\},$$
$$\mathcal{E}_{12} = \{(u^n(\tilde{m}_2, \tilde{m}_{1k}, \tilde{m}_r), v^n(\tilde{m}_2, \tilde{m}_{1k}, \tilde{m}_r, \tilde{m}_{1s}, \tilde{m}_{1r}), y_1^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } (\tilde{m}_2, \tilde{m}_{1k}, \tilde{m}_r) \neq (m_2, m_{1k}, m_r)\},$$
$$\mathcal{E}_{13} = \{(u^n(m_2, m_{1k}, m_r), v^n(m_2, m_{1k}, m_r, \tilde{m}_{1s}, \tilde{m}_{1r}), y_1^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{m}_{1s} \neq m_{1s}\}.$$

So $P_{e,1}$ can be upper bounded by

$$P_{e,1} \leq \Pr(\mathcal{E}_{11}) + \Pr(\mathcal{E}_{12}) + \Pr(\mathcal{E}_{13}).$$

By the LLN, $\Pr(\mathcal{E}_{11})$ tends to zero as $n \to \infty$. For $\Pr(\mathcal{E}_{12})$, since $u^n(\tilde{m}_2, \tilde{m}_{1k}, \tilde{m}_r)$ is independent of $(u^n(m_2, m_{1k}, m_r), y_1^n)$ for $(\tilde{m}_2, \tilde{m}_{1k}) \neq (m_2, m_{1k})$, by the packing lemma [19], $\Pr(\mathcal{E}_{12})$ tends to zero as $n \to \infty$ if

$$R_2 + R_{1k} + R_r + R_{1s} + R_{1r} \leq I(U, V_1; Y_1) - \delta_n(\epsilon_n). \tag{51}$$

For $\Pr(\mathcal{E}_{13})$, note that if $(\tilde{m}_{1s}, \tilde{m}_{1r}) \neq (m_{1s}, m_{1r})$, then for a given $u^n(m_2, m_{1k}, m_r)$, $v^n(m_2, m_{1k}, m_r, \tilde{m}_{1s}, \tilde{m}_{1r})$ is independent of $(v^n(m_2, m_{1k}, m_r, m_{1s}, m_{1r}), y_1^n)$. By the packing lemma [19], $\Pr(\mathcal{E}_{13})$ tends to zero as $n \to \infty$ if

$$R_{1s} + R_{1r} \leq I(V; Y_1|U) - \delta_n(\epsilon_n). \tag{52}$$

Analysis of individual secrecy: For the individual secrecy (3), i.e., $R_{L,i} \leq \tau_n$, for $i = 1, 2$, we show in the following its equivalent form that $H(M_i|Z^n) \geq nR_i - n\tau_n$.

First consider $H(M_2|Z^n)$. We have

$$\begin{aligned}
H(M_2|Z^n) =& H(M_2, Z^n) - H(Z^n) \\
=& H(U^n, M_2, Z^n) - H(U^n|M_2, Z^n) - H(Z^n) \\
=& H(U^n) + H(Z^n|U^n) - H(U^n|M_2, Z^n) - H(Z^n) \\
\overset{(a)}{\geq}& H(U^n) + H(Z^n|U^n) - n[R_{1k} + R_r - I(U; Z)] - H(Z^n) - n\tau_n/2 \\
\overset{(b)}{=}& n[R_2 + R_{1k} + R_r] - n[R_{1k} + R_r - I(U; Z)] - I(U^n; Z^n) - n\tau_n/2 \\
=& nR_2 + nI(U; Z) - I(U^n; Z^n) - n\tau_n/2 \\
\overset{(c)}{\geq}& nR_2 - n\tau_n
\end{aligned}$$

where (a) follows from [9, Lemma 1] that $H(U^n|M_2, Z^n) \leq n[R_{1k} + R_r - I(U; Z)] + n\tau_n/2$, if taking

$$R_{1k} + R_r \geq I(U; Z) + \delta_n(\tau_n); \tag{53}$$

(b) follows from the codebook construction that $H(U^n) = n[R_2 + R_{1k} + R_r]$; and (c) is due to the fact that $I(U^n; Z^n) \leq nI(U; Z) + n\tau_n/2$, the proof of which is given as follows.

$$\begin{aligned}
I(U^n; Z^n) =& H(Z^n) - H(Z^n|U^n) \\
=& H(Z^n) - H(Z^n|U^n, V^n) - I(V^n; Z^n|U^n) \\
\overset{(d)}{=}& H(Z^n) - nH(Z|U, V) - H(V^n|U^n) + H(V^n|U^n, Z^n) \\
\overset{(e)}{\leq}& H(Z^n) - nH(Z|U, V) - H(V^n|U^n) + n[R_{1s} + R_{1r} - I(V; Z|U)] + n\tau_n/2 \\
\overset{(f)}{\leq}& nH(Z) - nH(Z|U, V) - n[R_{1s} + R_{1r}] + n[R_{1s} + R_{1r} - I(V; Z|U)] + n\tau_n/2
\end{aligned}$$

$$=nI(U;Z)+n\tau_n/2,$$

where (d) is due to the discrete memoryless of the channel; (e) follows from [9, Lemma 1] that $H(V^n|U^n,Z^n)\leq n[R_{1s}+R_{1r}-I(V;Z|U)]+n\tau_n/2$, if taking

$$R_{1s}+R_{1r}\geq I(V;Z|U)+\delta_n(\tau_n); \tag{54}$$

(f) follows from the fact that $H(Z^n)=\sum_{i=1}^n H(Z_i|Z^{i-1})\leq\sum_{i=1}^n H(Z_i)=nH(Z)$ and by the codebook construction $H(V^n|U^n)=n[R_{1s}+R_{1r}]$.

For $H(M_1|Z^n)$, we have

$$\begin{aligned}
H(M_1|Z^n)=&H(M_{1k},M_{1s}|Z^n)\\
=&H(M_2,M_{1k},M_r,M_{1s}|Z^n)-H(M_2,M_r|M_{1k},M_{1s},Z^n)\\
=&H(U^n,M_{1s}|Z^n)-H(U^n|M_{1k},M_{1s},Z^n)\\
\overset{(g)}{\geq}&H(U^n|Z^n)+H(M_{1s}|U^n,Z^n)-H(U^n|M_{1k},Z^n)\\
=&H(U^n|Z^n)+H(V^n|U^n,Z^n)-H(V^n|M_{1s},U^n,Z^n)-H(U^n|M_{1k},Z^n)\\
\overset{(h)}{\geq}&H(U^n,V^n|Z^n)-n[R_{1r}-I(V;Z|U)]-n[R_2+R_r-I(U;Z)]-n\tau_n\\
=&H(U^n,V^n)-I(U^n,V^n;Z^n)-n[R_{1r}+R_2+R_r]+nI(U,V;Z)-n\tau_n\\
\overset{(i)}{\geq}&n[R_2+R_{1k}+R_r+R_{1s}+R_{1r}]-I(U^n,V^n;Z^n)-n[R_{1r}+R_2+R_r]+nI(U,V;Z)-n\tau_n\\
=&nR_1-I(U^n,V^n;Z^n)+nI(U,V;Z)-n\tau_n\\
\overset{(j)}{\geq}&nR_1-n\tau_n,
\end{aligned}$$

where (g) is due to the fact that conditioning reduces entropy; (h) follows from [9, Lemma 1] that by taking

$$R_2+R_r\geq I(U;Z)+\delta_n(\tau_n), \tag{55}$$

we have $H(U^n|M_{1k},Z^n)\leq n[R_2+R_r-I(U;Z)]+n\tau_n/2$; and by taking

$$R_{1r}\geq I(V;Z|U)+\delta_n(\tau_n), \tag{56}$$

we have $H(V^n|M_{1s},U^n,Z^n)\leq n[R_{1r}-I(V;Z|U)]+n\tau_n/2$; (i) is by the codebook construction that $H(U^n,V^n)=n[R_2+R_{1k}+R_r+R_{1s}+R_{1r}]$; (j) is due to the fact that $I(U^n,V^n;Z^n)\leq nI(U,V;Z)$, the proof of which is given as follows:

$$\begin{aligned}
I(U^n,V^n;Z^n)=&H(Z^n)-H(Z^n|U^n,V^n)\\
\overset{(k)}{=}&H(Z^n)-nH(Z|U,V)\\
\overset{(l)}{\leq}&nH(Z)-nH(Z|U,V)\\
=&nI(U,V;Z),
\end{aligned}$$

where (k) is due to the discrete memoryless of the channel; and (l) follows from the fact that $H(Z^n) = \sum_{i=1}^{n} H(Z_i|Z^{i-1}) \leq \sum_{i=1}^{n} H(Z_i) = nH(Z)$.

Achievable rate region: The resulting region has the following constraints: the non-negativity for rates, i.e., $R_{1k}, R_{1s}, R_r, R_{1r} \geq 0$, the rate relations imposed by rate splitting as specified in (49), the conditions for a reliable communication, i.e., (50), (51), (52), and the conditions for individual secrecy of the messages at the eavesdropper, i.e., (53), (54), (55), (56). Eliminating R_{1r}, R_r by applying Fourier-Motzkin procedure [19], we get the desired rate region as defined in (16); further eliminating R_{1s}, R_{1k}, we obtain (18).

Appendix D
Proof of Theorem 8

Consider a DM-BC with an external eavesdropper such that Y_2 is a degraded version of Y_1 and Y_2 is less noisy than Z. For a reliable communication under individual secrecy constraint, we have

$$\begin{aligned} nR_2 = H(M_2) &= I(M_2; Y_2^n) + H(M_2|Y_2^n) \\ &\overset{(a)}{\leq} I(M_2; Y_2^n) - I(M_2; Z^n) + n\lambda_2(\epsilon_n, \tau_n) \end{aligned} \tag{57}$$

where (a) is due to the reliability constraint (2) and individual secrecy constraint (3) and by taking $\lambda_2(\epsilon_n, \tau_n) = \tau_n + 1/n + \epsilon_n R_2$.

Moreover, we have

$$\begin{aligned} nR_1 =& H(M_1) = H(M_1|M_2) \\ =& I(M_1; Y_1^n|M_2) + H(M_1|M_2, Y_1^n) \\ \overset{(c)}{\leq}& \underbrace{I(M_1; Y_1^n|M_2) - I(M_1; Z^n|M_2)}_{nR_1^s} + \underbrace{I(M_1; Z^n|M_2)}_{nR_1^k} + n\lambda_1(\epsilon_n) \end{aligned} \tag{58}$$

where (c) is due to the reliability constraint (2) and Fano's inequality, the fact that $H(M_1|M_2, Y_1^n) \leq H(M_1|Y_1^n)$, and by taking $\lambda_1(\epsilon_n) = 1/n + \epsilon_n R_1$.

Note that for nR_1^k in (58), we have

$$\begin{aligned} nR_1^k =& I(M_1; Z^n|M_2) \\ =& I(M_1; Y_2^n|M_2) - I(M_1; Y_2^n|M_2) + I(M_1; Z^n|M_2) \\ =& I(M_1, M_2; Y_2^n) - I(M_2; Y_2^n) - I(M_1; Y_2^n|M_2) + I(M_1; Z^n|M_2) \\ \overset{(d)}{\leq}& I(M_1, M_2; Y_2^n) - I(M_1, M_2; Z^n) - I(M_1; Y_2^n|M_2) + I(M_1; Z^n|M_2) + n\lambda_2(\epsilon_n, \tau_n) \\ =& I(M_2; Y_2^n) - I(M_2; Z^n) + n\lambda_2(\epsilon_n, \tau_n) \end{aligned} \tag{59}$$

where (d) follows that $I(M_2; Y_2^n) \geq I(M_1, M_2; Z^n) - n\lambda_2(\epsilon_n, \tau_n)$, which proof is provided as follows:

$$I(M_2; Y_2^n) = H(M_2) - H(M_2|Y_2^n) \overset{(f)}{\geq} H(M_2) - n\lambda_2(\epsilon_n)$$

$$
\begin{aligned}
&= H(M_2|M_1) - n\lambda_2(\epsilon_n) \geq I(M_2; Z^n|M_1) - n\lambda_2(\epsilon_n) \\
&= I(M_1, M_2; Z^n) - I(M_1; Z^n) - n\lambda_2(\epsilon_n) \\
&\overset{(g)}{\geq} I(M_1, M_2; Z^n) - n\lambda_2(\epsilon_n, \tau_n)
\end{aligned}
$$

where (f) is due to the reliability constraint(2) and Fano's inequality and by taking $\lambda_2(\epsilon_n) = 1/n + \epsilon_n R_2$; and (g) is due to the individual secrecy constraint (3) and by taking $\lambda_2(\epsilon_n, \tau_n) = \tau_n + \lambda_2(\epsilon_n)$.

For $I(M_2; Y_2^n) - I(M_2; Z^n)$ in (57) and (59), we have

$$
\begin{aligned}
I(M_2;Y_2^n) - I(M_2; Z^n) &= \sum_{i=1}^{n} \left[I(M_2; Y_{2i}|Y_2^{i-1}) - I(M_2; Z_i|Z_{i+1}^n) \right] \\
&\overset{(h)}{=} \sum_{i=1}^{n} \left[I(M_2; Y_{2i}|Y_2^{i-1}) - I(M_2; Z_i|Z_{i+1}^n) \right] + \sum_{i=1}^{n} \left[I(Z_{i+1}^n; Y_{2i}|M_2, Y_2^{i-1}) - I(Y_2^{i-1}; Z_i|M_2, Z_{i+1}^n) \right] \\
&= \sum_{i=1}^{n} \left[I(M_2, Z_{i+1}^n; Y_{2i}|Y_2^{i-1}) - I(M_2, Y_2^{i-1}; Z_i|Z_{i+1}^n) \right] \\
&= \sum_{i=1}^{n} \left[I(M_2; Y_{2i}|Y_2^{i-1}, Z_{i+1}^n) - I(M_2; Z_i|Y_2^{i-1}, Z_{i+1}^n) \right] + \sum_{i=1}^{n} \left[I(Z_{i+1}^n; Y_{2i}|Y_2^{i-1}) - I(Y_2^{i-1}; Z_i|Z_{i+1}^n) \right] \\
&\overset{(h)}{=} \sum_{i=1}^{n} \left[I(M_2; Y_{2i}|Y_2^{i-1}, Z_{i+1}^n) - I(M_2; Z_i|Y_2^{i-1}, Z_{i+1}^n) \right] \\
&= \sum_{i=1}^{n} \left[I(M_2, Y_2^{i-1}, Z_{i+1}^n; Y_{2i}) - I(M_2, Y_2^{i-1}, Z_{i+1}^n; Z_i) \right] - \sum_{i=1}^{n} \left[I(Y_2^{i-1}, Z_{i+1}^n; Y_{2i}) - I(Y_2^{i-1}, Z_{i+1}^n; Z_i) \right] \\
&\overset{(i)}{\leq} \sum_{i=1}^{n} \left[I(M_2, Y_2^{i-1}, Z_{i+1}^n; Y_{2i}) - I(M_2, Y_2^{i-1}, Z_{i+1}^n; Z_i) \right] \\
&= \sum_{i=1}^{n} \left[I(M_2, Y_1^{i-1}, Y_2^{i-1}, Z_{i+1}^n; Y_{2i}) - I(M_2, Y_1^{i-1}, Y_2^{i-1}, Z_{i+1}^n; Z_i) \right] \\
&\quad - \sum_{i=1}^{n} \left[I(Y_1^{i-1}; Y_{2i}|M_2, Y_2^{i-1}, Z_{i+1}^n) - I(Y_1^{i-1}; Z_i|M_2, Y_2^{i-1}, Z_{i+1}^n) \right] \\
&\overset{(i)}{\leq} \sum_{i=1}^{n} \left[I(M_2, Y_1^{i-1}, Y_2^{i-1}, Z_{i+1}^n; Y_{2i}) - I(M_2, Y_1^{i-1}, Y_2^{i-1}, Z_{i+1}^n; Z_i) \right] \\
&\overset{(j)}{=} \sum_{i=1}^{n} \left[I(U_i; Y_{2i}) - I(U_i; Z_i) \right], \qquad (60)
\end{aligned}
$$

where (h) is due to the Csiszár sum identity; (i) is due to the fact that the channel to legitimate receiver 2 is less noisy than the one to the eavesdropper; and (j) is by setting $U_i = (M_2, Y_1^{i-1}, Y_2^{i-1}, Z_{i+1}^n)$.

Replacing (60) in (57) and (59), respectively, we obtain

$$
nR_2 \leq \sum_{i=1}^{n} I(U_i; Y_{2i}) - I(U_i; Z_i) + n\lambda_2(\epsilon_n, \tau_n); \qquad (61)
$$

$$
nR_1^k \leq \sum_{i=1}^{n} I(U_i; Y_{2i}) - I(U_i; Z_i) + n\lambda_2(\epsilon_n, \tau_n). \qquad (62)
$$

Similarly we bound R_1^s in (58) as follows:

$$\begin{aligned}
nR_1^s =& I(M_1;Y_1^n|M_2) - I(M_1;Z^n|M_2)\\
\overset{(k)}{=}& \sum_{i=1}^{n}\left[I(M_1;Y_{1i}|M_2,Y_1^{i-1},Z_{i+1}^n) - I(M_1;Z_i|M_2,Y_1^{i-1},Z_{i+1}^n)\right]\\
=& \sum_{i=1}^{n}\left[I(M_1,Y_2^{i-1};Y_{1i}|M_2,Y_1^{i-1},Z_{i+1}^n) - I(M_1,Y_2^{i-1};Z_i|M_2,Y_1^{i-1},Z_{i+1}^n)\right]\\
&- \sum_{i=1}^{n}\left[I(Y_2^{i-1};Y_{1i}|M_1,M_2,Y_1^{i-1},Z_{i+1}^n) - I(Y_2^{i-1};Z_i|M_1,M_2,Y_1^{i-1},Z_{i+1}^n)\right]\\
\leq& \sum_{i=1}^{n}\left[I(M_1,Y_2^{i-1};Y_{1i}|M_2,Y_1^{i-1},Z_{i+1}^n) - I(M_1,Y_2^{i-1};Z_i|M_2,Y_1^{i-1},Z_{i+1}^n)\right]\\
=& \sum_{i=1}^{n}\left[I(M_1;Y_{1i}|M_2,Y_1^{i-1},Y_2^{i-1},Z_{i+1}^n) - I(M_1;Z_i|M_2,Y_1^{i-1},Y_2^{i-1},Z_{i+1}^n)\right]\\
&+ \sum_{i=1}^{n}\left[I(Y_2^{i-1};Y_{1i}|M_2,Y_1^{i-1},Z_{i+1}^n) - I(Y_2^{i-1};Z_i|M_2,Y_1^{i-1},Z_{i+1}^n)\right]\\
\overset{(l)}{=}& \sum_{i=1}^{n}\left[I(M_1;Y_{1i}|M_2,Y_1^{i-1},Y_2^{i-1},Z_{i+1}^n) - I(M_1;Z_i|M_2,Y_1^{i-1},Y_2^{i-1},Z_{i+1}^n)\right]\\
\overset{(m)}{\leq}& \sum_{i=1}^{n}\left[I(V_i;Y_{1i}|U_i) - I(V_i;Z_i|U_i)\right] \qquad (63)
\end{aligned}$$

where (k) is obtained by applying the Csiszár sum identity twice; (l) is due to the channel degradedness that implies the Markov chains $Y_2^{i-1} \to (M_2, Y_1^{i-1}, Z_{i+1}^n) \to (Y_{1i}, Z_i)$; and (m) follows by the fact $U_i = (M_2, Y_1^{i-1}, Y_2^{i-1}, Z_{i+1}^n)$ and further setting $V_i = (M_1, U_i)$.

Replacing R_1^k and R_1^s in (58) by (62) and (63), respectively, we obtain

$$\begin{aligned}
nR_1 \leq& nR_1^k + nR_1^s + n\lambda_1(\epsilon_n)\\
\overset{(n)}{\leq}& \sum_{i=1}^{n}\left[I(V_i;Y_{1i}|U_i) - I(V_i;Z_i|U_i)\right] + \sum_{i=1}^{n}\left[I(U_i;Y_{2i}) - I(U_i;Z_i)\right] + n\lambda(\epsilon_n,\tau_n) \qquad (64)
\end{aligned}$$

where (n) is by taking $\lambda(\epsilon_n,\tau_n) = \lambda_1(\epsilon_n) + \lambda_2(\epsilon_n,\tau_n)$.

Now we proceed to bound $R_1 + R_2$.

$$\begin{aligned}
n(R_1+R_2) =& H(M_1|M_2) + H(M_2)\\
=& I(M_1;Y_1^n|M_2) + I(M_2;Y_2^n) + H(M_1|M_2,Y_1^n) + H(M_2|Y_2^n)\\
\overset{(o)}{\leq}& I(M_1;Y_1^n|M_2) + I(M_2;Y_2^n) + n\lambda(\epsilon_n)\\
=& I(M_1;Y_1^n|M_2) - I(M_1;Z^n|M_2) + I(M_2;Y_2^n) - I(M_2;Z^n) + I(M_1,M_2;Z^n) + n\lambda(\epsilon_n)\\
\overset{(p)}{\leq}& \sum_{i=1}^{n}\left[I(V_i;Y_{1i}|U_i) - I(V_i;Z_i|U_i)\right] + \sum_{i=1}^{n}\left[I(U_i;Y_{2i}) - I(U_i;Z_i)\right] + \sum_{i=1}^{n} I(M_1,M_2;Z_i|Z_{i+1}^n) + n\lambda(\epsilon_n)\\
\overset{(q)}{\leq}& \sum_{i=1}^{n}\left[I(V_i;Y_{1i}|U_i) - I(V_i;Z_i|U_i)\right] + \sum_{i=1}^{n}\left[I(U_i;Y_{2i}) - I(U_i;Z_i)\right] + \sum_{i=1}^{n} I(U_i,V_i;Z_i) + n\lambda(\epsilon_n)
\end{aligned}$$

$$= \sum_{i=1}^{n} [I(V_i; Y_{1i}|U_i) + I(U_i; Y_{2i})] + n\lambda(\epsilon_n) \tag{65}$$

where (o) is due to the reliability constraint (2) and Fano's inequality, the fact that $H(M_1|M_2, Y_1^n) \leq H(M_1|Y_1^n)$ and by taking $\lambda(\epsilon_n) = 2/n + \epsilon_n(R_1 + R_2)$; (p) is due to (60) and (63); and (q) is due to the definition of U_i and V_i, i.e., $U_i = (M_2, Y_1^{i-1}, Y_2^{i-1}, Z_{i+1}^n)$ and $V_i = (M_1, U_i)$.

Introducing a time-sharing random variable Q which is uniform over $1, 2 \cdots, n$ and taking $U = (U_Q, Q), V = V_Q, Y_1 = Y_{1,Q}, Y_2 = Y_{2,Q}, Z = Z_Q$, we proceed on (61), (64) and (65) as follows:

$$\begin{aligned} R_2 &\leq I(U; Y_2) - I(U; Z) + \lambda_2(\epsilon_n, \tau_n) \\ R_1 &\leq I(V; Y_1|U) - I(V; Z|U) + I(U; Y_2) - I(U; Z) + \lambda(\epsilon_n, \tau_n) \\ R_1 + R_2 &\leq I(V; Y_1|U) + I(U; Y_2) + \lambda(\epsilon_n) \end{aligned}$$

Taking the limit as $n \to \infty$ such that $\lambda_2(\epsilon_n, \tau_n), \lambda(\epsilon_n, \tau_n), \lambda(\epsilon_n) \to 0$, we conclude our proof of the upper bound.

Appendix E
Proof of Theorem 10

For a given input probability distribution $p(u, v_1, v_2, x)$, let $I_1 = I(V; Y_1|U) - I(V; Z|U)$ and $I_2 = I(V; Y_2|U) - I(V; Z|U)$. If $I_1, I_2 \leq 0$, the claimed region (26) reduces to (14), which is achievable by taking the primitive approach as described in Section IV-A. We assume $I_1 > 0$. Now, if $I_2 \leq 0$, the claimed region (26) reduces to (18), which is achievable by employing the superposition approach as described in Section IV-B. A similar proof applies to the case of $I_1 \leq 0$ and $I_2 > 0$. In the following, we provide the detailed achievability proof for the remaining case, i.e., if $I_1 > 0$ and $I_2 > 0$ for a given $p(u, v_1, v_2, x)$.

Rate splitting: As illustrated in Fig. 12, we represent M_1, M_2 by $M_1 = (M_{1k}, M_{1s})$ and $M_2 = (M_{2k}, M_{2s})$ with M_{1k}, M_{2k} of entropy nR_{1k}, nR_{2k}, respectively; while M_{1s}, M_{2s} of entropy nR_{1s}, nR_{2s}, respectively. Therefore, we have

$$R_1 = R_{1k} + R_{1s}; \tag{66}$$

$$R_2 = R_{2k} + R_{2s}. \tag{67}$$

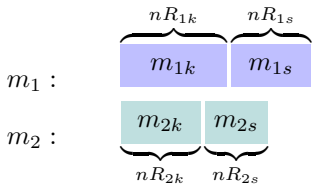


Fig. 12: Marton's coding: Rate splitting.

Codebook generation: Fix $p(u), p(v_1, v_2|u)$.

First, randomly generate $2^{n(R_{1k}+R_{2k}+R_r)}$ i.i.d. sequences $u^n(m_{2k}, m_{1k}, m_r)$, with $(m_{2k}, m_{1k}, m_r) \in [1 : 2^{nR_{2k}}] \times [1 : 2^{nR_{1k}}] \times [1 : 2^{nR_r}]$, according to $p(u)$.

For each fixed $u^n(m_{2k}, m_{1k}, m_r)$, randomly generate $2^{n(R_{1s}+R_{1r}+R_{1c})}$ i.i.d. sequences $v_1^n(m_{2k}, m_{1k}, m_r, m_{1s}, m_{1r}, m_{1c})$ with $(m_{1s}, m_{1r}, m_{1c}) \in [1 : 2^{nR_{1s}}] \times [1 : 2^{nR_{1r}}] \times [1 : 2^{nR_{1c}}]$, according to $p(v_1|u)$; and similarly generate $2^{n(R_{2s}+R_{2r}+R_{2c})}$ i.i.d. sequences $v_2^n(m_{2k}, m_{1k}, m_r, m_{2s}, m_{2r}, m_{2c})$ with $(m_{2s}, m_{2r}, m_{2c}) \in [1 : 2^{nR_{2s}}] \times [1 : 2^{nR_{2r}}] \times [1 : 2^{nR_{2c}}]$, according to $p(v_2|u)$.

Encoding: To send messages (m_1, m_2), with $m_1 = (m_{1k}, m_{1s})$, $m_2 = (m_{2k}, m_{2s})$, randomly choose $m_r \in [1 : 2^{nR_r}]$ and find $u^n(m_{2k}, m_{1k}, m_r)$.

Given $u^n(m_{2k}, m_{1k}, m_r)$, randomly choose $(m_{1r}, m_{2r}) \in [1 : 2^{nR_{1r}}] \times [1 : 2^{nR_{2r}}]$, and pick (m_{1c}, m_{2c}) such that $v_1^n(m_{2k}, m_{1k}, m_r, m_{1s}, m_{1r}, m_{1c})$ and $v_1^n(m_{2k}, m_{1k}, m_r, m_{2s}, m_{2r}, m_{2c})$ are jointly typical. (If there is more than one such jointly typical pair, choose one of them uniformly at random.) This is possible with high probability, if

$$R_{1c} + R_{2c} > I(V_1; V_2|U) \tag{68}$$

(refer to [6] for the proof).

Finally, for the chosen jointly typical pair (v_1^n, v_2^n), generate a codeword x^n at random according to $p(x|v_1, v_2)$ and transmit it.

The choice of u^n, v_1^n, v_2^n, x^n for given (m_1, m_2) is illustrated in Fig. 13.

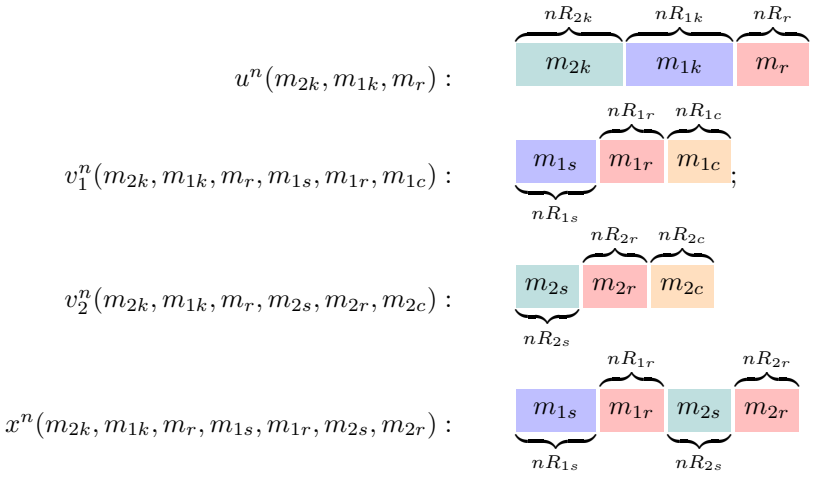


Fig. 13: Marton's coding: Encoding.

Decoding: Receiver 1, upon receiving y_1^n, finds a unique tuple $(\hat{m}_{2k}, \hat{m}_{1k}, \hat{m}_r, \hat{m}_{1s})$ such that $(u^n(\hat{m}_{2k}, \hat{m}_{1k}, \hat{m}_r), v_1^n(\hat{m}_{2k}, \hat{m}_{1k}, \hat{m}_r, \hat{m}_{1s}, \hat{m}_{1r}, \hat{m}_{1c})$ is jointly typical with y_1^n for some $(\hat{m}_{1r}, \hat{m}_{1c})$. And, receiver 2, upon receiving y_2^n, finds a unique tuple $(\tilde{m}_{2k}, \tilde{m}_{1k}, \tilde{m}_r, \tilde{m}_{2s})$ such that $(u^n(\tilde{m}_{2k}, \tilde{m}_{1k}, \tilde{m}_r), v_2^n(\tilde{m}_{2k}, \tilde{m}_{1k}, \tilde{m}_r, \tilde{m}_{2s}, \tilde{m}_{2r}, \tilde{m}_{2c}))$ is jointly typical with y_2^n for some $(\tilde{m}_{2r}, \tilde{m}_{2c})$.

Analysis of the error probability of decoding: Assume that $m_1 = (m_{1k}, m_{1s})$, $m_2 = (m_{2k}, m_{2s})$ is sent.

For $P_{e,1}$, a decoding error happens if receiver 1's estimate is $(u^n(\hat{m}_{2k}, \hat{m}_{1k}, \hat{m}_r), v_1^n(\hat{m}_{2k}, \hat{m}_{1k}, \hat{m}_r, \hat{m}_{1s}, \hat{m}_{1r}, \hat{m}_{1c}))$ with $(\hat{m}_{2k}, \hat{m}_{1k}, \hat{m}_r, \hat{m}_{1s}) \neq (m_{2k}, m_{1k}, m_r, m_{1s})$. In more details, the error event can be partitioned into the followings:

1) Error event corresponds to $(\hat{m}_{2k}, \hat{m}_{1k}, \hat{m}_r) \neq (m_{2k}, m_{1k}, m_r)$. Note that this event occurs with arbitrarily small probability (e.g.: $\epsilon_n/2$) if

$$R_{1k} + R_{2k} + R_r + R_{1s} + R_{1r} + R_{1c} \leq I(U, V_1; Y_1) - \delta_n(\epsilon_n). \tag{69}$$

2) Error event corresponds to $(\hat{m}_{2k}, \hat{m}_{1k}, \hat{m}_r) = (m_{2k}, m_{1k}, m_r)$ but $\hat{m}_{1s} \neq m_{1s}$. Note that this event occurs with arbitrarily small probability (e.g.: $\epsilon_n/2$) if

$$R_{1s} + R_{1r} + R_{1c} \leq I(V_1; Y_1|U) - \delta_n(\epsilon_n). \tag{70}$$

Similar analysis can be done at the receiver 2, from which the decoding error probability $P_{e,2}$ can be made arbitrarily small (e.g.: ϵ_n) if

$$R_{1k} + R_{2k} + R_r + R_{2s} + R_{2r} + R_{2c} \leq I(U, V_2; Y_2) - \delta_n(\epsilon_n); \tag{71}$$

$$R_{2s} + R_{2r} + R_{2c} \leq I(V_2; Y_2|U) - \delta_n(\epsilon_n). \tag{72}$$

Analysis of individual secrecy: For the individual secrecy (3), i.e., $R_{L,i} \leq \tau_n$, for $i = 1, 2$, it suffices to show that $H(M_1|Z^n) + H(M_2|Z^n) \geq H(M_1) + H(M_2) - n\tau_n = n(R_1 + R_2) - n\tau_n$.

First consider $H(M_1|Z^n)$, we have

$$\begin{aligned}
H(M_1|Z^n) =& H(M_{1k}, M_{1s}|Z^n) \\
=& H(M_{1k}, M_{2k}, M_r, M_{1s}|Z^n) - H(M_{2k}, M_r|M_{1k}, M_{1s}, Z^n) \\
=& H(U^n, M_{1s}|Z^n) - H(U^n|M_{1k}, M_{1s}, Z^n) \\
\overset{(a)}{\geq}& H(U^n|Z^n) + H(M_{1s}|U^n, Z^n) - H(U^n|M_{1k}, Z^n) \\
\overset{(b)}{\geq}& H(U^n|Z^n) + H(M_{1s}|U^n, Z^n) - n[R_{2k} + R_r - I(U; Z)] - n\tau_n/6 \\
=& H(U^n|Z^n) + H(V_1^n, M_{1s}|U^n, Z^n) - H(V_1^n|M_{1s}, U^n, Z^n) - n[R_{2k} + R_r - I(U; Z)] - n\tau_n/6 \\
\overset{(b)}{\geq}& H(U^n|Z^n) + H(V_1^n|U^n, Z^n) - n[R_{1r} + R_{1c} - I(V_1; Z|U)] - n[R_{2k} + R_r - I(U; Z)] - n\tau_n/3 \\
=& H(U^n, V_1^n|Z^n) - n[R_{1r} + R_{1c} - I(V_1; Z|U)] - n[R_{2k} + R_r - I(U; Z)] - n\tau_n/3
\end{aligned} \tag{73}$$

where (a) is due to the fact that conditioning reduces entropy; (b) follows from [9, Lemma 1] that we have

- $H(U^n|M_{1k}, Z^n) \leq n[R_{2k} + R_r - I(U; Z)] + n\tau_n/6$ if taking

$$R_{2k} + R_r \geq I(U; Z) + \delta_n(\tau_n); \tag{74}$$

- $H(V_1^n|M_{1s}, U^n, Z^n) \leq n[R_{1r} + R_{1c} - I(V_1; Z|U)] + n\tau_n/6$ if taking

$$R_{1r} + R_{1c} \geq I(V_1; Z|U) + \delta_n(\tau_n). \tag{75}$$

Similarly, we could show that

$$\begin{aligned} H(M_2|Z^n) =& H(M_{2k}, M_{2s}|Z^n) \\ \geq& H(U^n, V_2^n|Z^n) - n[R_{2r} + R_{2c} - I(V_2; Z|U)] - n[R_{1k} + R_r - I(U; Z)] - n\tau_n/3 \end{aligned} \tag{76}$$

if taking

$$R_{1k} + R_r \geq I(U; Z) + \delta_n(\tau_n); \tag{77}$$

$$R_{2r} + R_{2c} \geq I(V_2; Z|U) + \delta_n(\tau_n). \tag{78}$$

Note that

$$\begin{aligned} & H(U^n, V_1^n|Z^n) + H(U^n, V_2^n|Z^n) \\ &= 2H(U^n|Z^n) + H(V_1^n|U^n, Z^n) + H(V_2^n|U^n, Z^n) \\ &\geq 2H(U^n|Z^n) + H(V_1^n, V_2^n|U^n, Z^n) \\ &= 2H(U^n) - 2I(U^n; Z^n) + H(V_1^n, V_2^n, Z^n|U^n) - H(Z^n|U^n) \\ &= 2H(U^n) - 2I(U^n; Z^n) + H(V_1^n, V_2^n|U^n) + H(Z^n|U^n, V_1^n, V_2^n) - H(Z^n|U^n) \\ &\overset{(d)}{\geq} 2H(U^n) - 2I(U^n; Z^n) + H(V_1^n, V_2^n|U^n) - nI(V_1, V_2; Z|U) \\ &\overset{(e)}{\geq} 2n[R_{2k} + R_{1k} + R_r] + n[R_{1s} + R_{1r} + R_{2s} + R_{2r}] - 2I(U^n; Z^n) - nI(V_1, V_2; Z|U) \\ &\overset{(f)}{\geq} 2n[R_{2k} + R_{1k} + R_r] + n[R_{1s} + R_{1r} + R_{2s} + R_{2r}] - 2nI(U; Z) - nI(V_1, V_2; Z|U) - n\tau_n/3 \end{aligned} \tag{79}$$

where (d) follows from the fact that $H(Z^n|U^n, V_1^n, V_2^n) = nH(Z|U, V_1, V_2)$ due to the discrete memoryless of the channel and $H(Z^n|U^n) = \sum_{i=1}^n H(Z_i|U^n, Z^{i-1}) \leq \sum_{i=1}^n H(Z_i|U_i) = nH(Z|U)$; (e) follows from the codebook construction that $H(U^n) = n[R_{2k} + R_{1k} + R_r]$ and $H(V_1^n, V_2^n|U^n) \geq n[R_{1s} + R_{1r} + R_{2s} + R_{2r}]$; and (f) is due to the fact that $I(U^n; Z^n) \leq nI(U; Z) + n\tau_n/6$, the proof of which is given as follows:

$$\begin{aligned} I(U^n; Z^n) =& H(Z^n) - H(Z^n|U^n) \\ =& H(Z^n) - H(Z^n|U^n, V_1^n, V_2^n) - I(V_1^n, V_2^n; Z^n|U^n) \\ \overset{(g)}{=}& H(Z^n) - nH(Z|U, V_1, V_2) - H(V_1^n, V_2^n|U^n) + H(V_1^n, V_2^n|U^n, Z^n) \\ \overset{(h)}{\leq}& H(Z^n) - nH(Z|U, V_1, V_2) - H(V_1^n, V_2^n|U^n) + H(V_1^n|U^n, Z^n) + H(V_2^n|U^n, Z^n) \\ \overset{(i)}{\leq}& H(Z^n) - nH(Z|U, V_1, V_2) - H(V_1^n, V_2^n|U^n) \\ & + n[R_{1s} + R_{1r} + R_{1c} - I(V_1; Z|U)] + n[R_{2s} + R_{2r} + R_{2c} - I(V_2; Z|U)] + n\tau_n/6 \\ \overset{(j)}{\leq}& nH(Z) - nH(Z|U, V_1, V_2) - n[R_{1s} + R_{1r} + R_{2s} + R_{2r}] \\ & + n[R_{1s} + R_{1r} + R_{1c} - I(V_1; Z|U)] + n[R_{2s} + R_{2r} + R_{2c} - I(V_2; Z|U)] + n\tau_n/6 \\ =& nI(U; Z) + n[R_{1c} + R_{2c} + I(V_1; V_2; Z|U) - I(V_1; Z|U) - I(V_2; Z|U)] + n\tau_n/6 \end{aligned}$$

$$\overset{(k)}{\leq} nI(U;Z) + n\tau_n/6$$

where (g) is due to the discrete memoryless of the channel; (h) follows the fact that $H(A,B|C) \leq H(A|C) + H(B|C)$; (i) follows from [9, Lemma 1] that we have

- $H(V_1^n|U^n,Z^n) \leq n[R_{1s}+R_{1r}+R_{1c}-I(V_1;Z|U)]+n\tau_n/12$ if taking

$$R_{1s}+R_{1r}+R_{1c} \geq I(V_1;Z|U)+\delta_n(\tau_n). \tag{80}$$

  (Note that (80) holds if (75) holds.)

- $H(V_2^n|U^n,Z^n) \leq n[R_{2s}+R_{2r}+R_{2c}-I(V_2;Z|U)]+n\tau_n/12$ if taking

$$R_{2s}+R_{2r}+R_{2c} \geq I(V_2;Z|U)+\delta_n(\tau_n). \tag{81}$$

  (Note that (81) holds if (78) holds.)

(j) follows from the fact that $H(Z^n) = \sum_{i=1}^n H(Z_i|Z^{i-1}) \leq \sum_{i=1}^n H(Z_i) = nH(Z)$ and by the codebook construction $H(V_1^n,V_2^n|U^n) \geq n[R_{1s}+R_{1r}+R_{2s}+R_{2r}]$; and (k) is by taking

$$R_{1c}+R_{2c} \leq I(V_1;Z|U)+I(V_2;Z|U)-I(V_1,V_2;Z|U). \tag{82}$$

Combining (73) and (76), we obtain

$$\begin{aligned}
H(M_1|Z^n)+H(M_2|Z^n) &\overset{(l)}{\geq} H(U^n,V_1^n|Z^n)-n[R_{1r}+R_{1c}-I(V_1;Z|U)]-n[R_{2k}+R_r-I(U;Z)]-n\tau_n/3 \\
&\quad + H(U^n,V_2^n|Z^n)-n[R_{2r}+R_{2c}-I(V_2;Z|U)]-n[R_{1k}+R_r-I(U;Z)]-n\tau_n/3 \\
&\overset{(m)}{\geq} n[R_1+R_2]-n[R_{1c}+R_{2c}]+n[I(V_1;Z|U)+I(V_2;Z|U)-I(V_1,V_2;Z|U)]-n\tau_n \\
&\overset{(n)}{\geq} n[R_1+R_2]-n\tau_n,
\end{aligned}$$

where (l) is due to (73) and (76); (m) is according to (79) and the fact that $R_1 = R_{1k}+R_{1s}$ and $R_2 = R_{2k}+R_{2s}$ as defined in (66) and (67), respectively; and (n) is due to (82).

Achievable rate region: We summarize the rate requirements in order to guarantee a reliable communication to both legitimate receivers and satisfy the individual secrecy constraints at the eavesdropper as follows:

- the non-negativity for rates, i.e.,

$$R_{1k},R_{2k},R_{1s},R_{2s},R_r,R_{1r},R_{2r},R_{1c},R_{2c} \geq 0;$$

- the rate relations imposed by rate splitting as specified in (66) and (67), i.e.,

$$R_1 = R_{1k}+R_{1s};$$

$$R_2 = R_{2k}+R_{2s}.$$

- the conditions for a reliable communication to both legitimate receivers, i.e., (68), (69), (70), (71), (72):

$$R_{1c}+R_{2c} > I(V_1;V_2|U) \tag{83}$$

$$R_{1k}+R_{2k}+R_r+R_{1s}+R_{1r}+R_{1c} \leq I(U,V_1;Y_1) \tag{84}$$

$$R_{1s} + R_{1r} + R_{1c} \leq I(V_1; Y_1|U) \tag{85}$$

$$R_{1k} + R_{2k} + R_r + R_{2s} + R_{2r} + R_{2c} \leq I(U, V_2; Y_2) \tag{86}$$

$$R_{2s} + R_{2r} + R_{2c} \leq I(V_2; Y_2|U) \tag{87}$$

- the conditions for individual secrecy of the messages at the eavesdropper, i.e., (74), (75), (77), (78), (82):

$$R_{2k} + R_r \geq I(U; Z) \tag{88}$$

$$R_{1r} + R_{1c} \geq I(V_1; Z|U) \tag{89}$$

$$R_{1k} + R_r \geq I(U; Z) \tag{90}$$

$$R_{2r} + R_{2c} \geq I(V_2; Z|U) \tag{91}$$

$$R_{1c} + R_{2c} \leq I(V_1; Z|U) + I(V_2; Z|U) - I(V_1, V_2; Z|U) \tag{92}$$

  Note that (88) and (90) can be replaced by the following inequality

$$\min\{R_{1k}, R_{2k}\} + R_r \geq I(U; Z). \tag{93}$$

Eliminating $R_r, R_{1r}, R_{2r}, R_{1c}, R_{2c}$ by applying Fourier-Motzkin procedure [19], we obtain the region of $(R_1, R_2) = (R_{1k} + R_{1s}, R_{2k} + R_{2s})$ in terms of $(R_{1k}, R_{1s}, R_{2k}, R_{2s})$ as given in (24) in Theorem 10. Note that a sketch of this Fourier-Motzkin procedure is provided in Appendix F. Further eliminate $R_{1k}, R_{1s}, R_{2k}, R_{2s}$, one can derive the same region in terms of (R_1, R_2) as given in (26) in Theorem 10.

Appendix F
Fourier-Motzkin Elimination for Theorem 10

Here we briefly outline the Fourier-Motzkin procedure in the proof of Theorem 10.

- To eliminate R_r, we consider the non-negativity of the rate R_r and the inequalities (84), (86) and (93) which involve R_r. We end up with

$$R_k + R_{1s} + R_{1r} + R_{1c} \leq I(U, V_1; Y_1) \tag{94}$$

$$R_k + R_{2s} + R_{2r} + R_{2c} \leq I(U, V_2; Y_2), \tag{95}$$

  where $R_k = \max\left\{R_{1k} + R_{2k}, \max\{R_{1k}, R_{2k}\} + I(U; Z)\right\}$.

- To eliminate R_{1r}, we consider the non-negativity of the rate R_{1r} and the inequalities (85), (89) and (94) which involve R_{1r}. We end up with

$$R_{1s} + R_{1c} \leq I(V_1; Y_1|U) \tag{96}$$

$$R_k + R_{1s} + R_{1c} \leq I(U, V_1; Y_1) \tag{97}$$

$$R_{1s} \leq I(V_1; Y_1|U) - I(V_1; Z|U) \tag{98}$$

$$R_k + R_{1s} \leq I(U, V_1; Y_1) - I(V_1; Z|U) \tag{99}$$

- To eliminate R_{2r}, we consider the non-negativity of the rate R_{2r} and the inequalities (87), (91) and (95) which involve R_{2r}. We end up with

$$R_{2s} + R_{2c} \leq I(V_2; Y_2|U) \tag{100}$$

$$R_k + R_{2s} + R_{2c} \leq I(U, V_2; Y_2) \tag{101}$$

$$R_{2s} \leq I(V_2; Y_2|U) - I(V_2; Z|U) \tag{102}$$

$$R_k + R_{2s} \leq I(U, V_2; Y_2) - I(V_2; Z|U) \tag{103}$$

- To eliminate R_{1c}, we consider the non-negativity of the rate R_{1c} and the inequalities (83), (92), (96) and (97) which involve R_{1c}. We end up with the following inequalities after canceling the redundant ones.

$$I(V_1; V_2|U) \leq I(V_1; Z|U) + I(V_2; Z|U) - I(V_1, V_2; Z|U) \tag{104}$$

$$R_{2c} \leq I(V_1; Z|U) + I(V_2; Z|U) - I(V_1, V_2; Z|U) \tag{105}$$

$$R_{2c} - R_{1s} \geq I(V_1; V_2|U) - I(V_1; Y_1|U) \tag{106}$$

$$R_{2c} - R_k - R_{1s} \geq I(V_1; V_2|U) - I(U, V_1; Y_1) \tag{107}$$

- To eliminate R_{2c}, we consider the non-negativity of the rate R_{2c} and the inequalities (100), (101), (105), (106) and (107) which involve R_{2c}. All the resulting inequalities are redundant (i.e., they all can be derived by combinations of other existing inequalities). Thus no new inequalities are introduced.

So far, we have for R_{1s}, R_{2s} the inequalities (98) and (102), respectively; and for their combinations with R_{1k}, R_{2k} (implied by R_k) the inequalities (99) and (103). Additionally, the inequality (104) need to be fulfilled by the choices of (U, V_1, V_2). This yields the desired region in terms of $(R_{1k}, R_{1s}, R_{2k}, R_{2s})$ as given in (24) in Theorem 10.

Appendix G
Proof of Theorem 11

In this appendix, we establish the rate region as given in Theorem 11 under the *joint* secrecy constraint. To this end, we utilize the same encoding and decoding schemes as described in Appendix E. As a direct consequence, the reliability proof (i.e., analysis of the error probability of decoding) remains the same. However, we need to revise the secrecy analysis under the joint secrecy constraint. That is, the achievability scheme needs to fulfill the joint secrecy constraint (5), unlike the analysis given in Appendix E, in which the individual secrecy constraint (3) is satisfied.

Analysis of joint secrecy: For the joint secrecy (5), i.e., $R_L \leq \tau_n$, it is equivalent to show that $H(M_1, M_2|Z^n) \geq H(M_1, M_2) - n\tau_n = n(R_1 + R_2) - n\tau_n$.

$H(M_1, M_2|Z^n) = H(M_{1k}, M_{2k}, M_{1s}, M_{2s}|Z^n)$

$$
\begin{aligned}
&=H(M_{1k},M_{2k},M_{1s},M_{2s},M_r|Z^n)-H(M_r|M_{1k},M_{2k},M_{1s},M_{2s},Z^n)\\
&=H(U^n,M_{1s},M_{2s}|Z^n)-H(U^n|M_{1k},M_{2k},M_{1s},M_{2s},Z^n)\\
&\geq H(U^n,M_{1s},M_{2s}|Z^n)-H(U^n|M_{1k},M_{2k},Z^n)\\
&=H(U^n,V_1^n,V_2^n|Z^n)-H(M_{1r},M_{1c},M_{2r},M_{2c}|U^n,M_{1s},M_{2s},Z^n)-H(U^n|M_{1k},M_{2k},Z^n)\\
&\overset{(a)}{\geq} H(U^n,V_1^n,V_2^n|Z^n)-H(U^n|M_{1k},M_{2k},Z^n)\\
&\quad -H(M_{1r},M_{1c}|U^n,M_{1s},M_{2s},Z^n)-H(M_{2r},M_{2c}|U^n,M_{1s},M_{2s},Z^n)\\
&\overset{(b)}{\geq} H(U^n,V_1^n,V_2^n|Z^n)-H(U^n|M_{1k},M_{2k},Z^n)\\
&\quad -H(M_{1r},M_{1c}|U^n,M_{1s},Z^n)-H(M_{2r},M_{2c}|U^n,M_{2s},Z^n)\\
&=H(U,V_1^n,V_2^n)-H(Z^n)+H(Z^n|U^n,V_1^n,V_2^n)-H(U^n|M_{1k},M_{2k},Z^n)\\
&\quad -H(V_1^n|U^n,M_{1s},Z^n)-H(V_2^n|U^n,M_{2s},Z^n)\\
&\overset{(c)}{\geq} n[R_{1k}+R_{2k}+R_r+R_{1s}+R_{2s}+R_{1r}+R_{2r}]-nI(U,V_1,V_2;Z)-n[R_r-I(U;Z)]\\
&\quad -n[R_{1r}+R_{1c}-I(V_1;Z|U)]-n[R_{2r}+R_{2c}-I(V_2;Z|U)]-n\tau_n\\
&\overset{(d)}{\geq} n[R_1+R_2]-n\tau_n
\end{aligned}
$$

where (a) follows from the fact that $H(A,B|C)\leq H(A|C)+H(B|C)$; (b) is due to the fact that conditioning reduces entropy; (c) follows from that

1) $H(U^n)=n[R_{2k}+R_{1k}+R_r]$ and $H(V_1^n,V_2^n|U^n)\geq n[R_{1s}+R_{1r}+R_{2s}+R_{2r}]$ by the codebook construction;
2) $H(Z^n)=\sum_{i=1}^n H(Z_i|Z^{i-1})\leq\sum_{i=1}^n H(Z_i)=nH(Z|U)$;
3) $H(Z^n|U^n,V_1^n,V_2^n)=nH(Z|U,V_1,V_2)$ due to the discrete memoryless of the channel;
4) applying [9, Lemma 1], we have that
   - $H(U^n|M_{1k},M_{2k},Z^n)\leq n[R_r-I(U;Z)]+n\tau_n/3$ if taking
   $$R_r\geq I(U;Z)+\delta_n(\tau_n); \tag{108}$$
   - $H(V_1^n|M_{1s},U^n,Z^n)\leq n[R_{1r}+R_{1c}-I(V_1;Z|U)]+n\tau_n/3$ if taking (75), i.e.,
   $$R_{1r}+R_{1c}\geq I(V_1;Z|U)+\delta_n(\tau_n);$$
   - $H(V_2^n|M_{2s},U^n,Z^n)\leq n[R_{2r}+R_{2c}-I(V_1;Z|U)]+n\tau_n/3$ if taking (78), i.e.,
   $$R_{2r}+R_{2c}\geq I(V_2;Z|U)+\delta_n(\tau_n);$$

(d) is by taking (82), i.e.,

$$R_{1c}+R_{2c}\leq I(V_1;Z|U)+I(V_2;Z|U)-I(V_1,V_2;Z|U).$$

We note that a stronger constraint (108) is imposed on R_r in order to guarantee the joint secrecy, instead of the (74) and (77) for the case of individual secrecy.

Achievable rate region: The resulting region has the following constraints: the non-negativity for rates, i.e., $R_{1k}, R_{2k}, R_{1s}, R_{2s}, R_r, R_{1r}, R_{2r}, R_{1c}, R_{2c} \geq 0$, the rate relations imposed by rate splitting as specified in (66) and (67), the conditions for a reliable communication to both legitimate receivers, i.e., (68), (69), (70), (71), (72), and the conditions for joint secrecy of the messages at the eavesdropper, i.e., (108), (75), (78), (82). Eliminating $R_{1k}, R_{2k}, R_{1s}, R_{2s}, R_{1c}, R_{2c}, R_{1r}, R_{2r}, R_r$ by applying Fourier-Motzkin procedure [19], we obtain the region of (R_1, R_2) as given in (27) in Theorem 11.

Appendix H
Proof of (36)

Recall Costa's EPI as described in the following.

Lemma 19. *[32, Theorem 1] Let X be an arbitrarily distributed n-dimensional random variable. Let N be a n-dimensional Gaussian vector, independent of X, and with covariance matrix proportional to the identity matrix, then*

$$e^{\frac{2}{n}h(X+\beta N)} \geq (1-\beta^2)e^{\frac{2}{n}h(X)} + \beta^2 e^{\frac{2}{n}h(X+N)}, \tag{109}$$

where $\beta \in [0,1]$.

Consider the Gaussian DBC under our investigation. Due to the degradedness order $Y_1^n \to Y_2^n \to Z^n$, we could write

$$Y_2^n = Y_1^n + \beta(N_{12}^n + N_{2e}^n),$$
$$Z^n = Y_1^n + N_{12}^n + N_{2e}^n,$$

where $N_{12}^n \sim \mathcal{N}(\mathbf{0}, (\sigma_2^2 - \sigma_1^2)\mathbf{I})$ and $N_{2e} \sim \mathcal{N}(\mathbf{0}, (\sigma_2^2 - \sigma_1^2)\mathbf{I})$, and

$$\beta = \sqrt{\frac{\sigma_2^2 - \sigma_1^2}{\sigma_e^2 - \sigma_1^2}}. \tag{110}$$

Note that N_{12}^n, N_{2e}^n are independent of Y_1^n and M_2.

Now applying Costa's EPI as described in (109), we have

$$e^{\frac{2}{n}h(Y_2^n|M_2)} \geq (1-\beta^2)e^{\frac{2}{n}h(Y_1^n|M_2)} + \beta^2 e^{\frac{2}{n}h(Z^n)}.$$

Dividing both sides by $e^{\frac{2}{n}h(Z^n)}$, we obtain

$$e^{\frac{2}{n}[h(Y_2^n|M_2)-h(Z^n|M_2)]} \geq (1-\beta^2)e^{\frac{2}{n}[h(Y_1^n|M_2)-h(Z^n|M_2)]} + \beta^2.$$

Replacing $h(Y_2^n|M_2) - h(Z^n|M_2)$ and β by their realizations as specified in (33) and (110), respectively, we obtain

$$\frac{\alpha P + \sigma_2^2}{\alpha P + \sigma_e^2} \geq \frac{\sigma_e^2 - \sigma_2^2}{\sigma_e^2 - \sigma_1^2} e^{\frac{2}{n}[h(Y_1^n|M_2)-h(Z^n|M_2)]} + \frac{\sigma_2^2 - \sigma_1^2}{\sigma_e^2 - \sigma_1^2}.$$

Easy calculation gives

$$h(Y_1^n|M_2) - h(Z^n|M_2) \leq \frac{n}{2}\log\frac{\alpha P + \sigma_1^2}{\alpha P + \sigma_e^2},$$

i.e., (36). This concludes our proof.

Appendix I
Proof of (38)

Recall Shannon's EPI as described in the following.

Lemma 20. *[33] For any two independent, n-dimensional random variable X and N,*

$$e^{\frac{2}{n}h(X+N)} \geq e^{\frac{2}{n}h(X)} + e^{\frac{2}{n}h(N)}. \tag{111}$$

Consider the Gaussian DBC under our investigation. We could write

$$Z^n = Y_1^n + N_{1e}^n,$$

where $N_{1e}^n \sim \mathcal{N}(\mathbf{0}, (\sigma_e^2 - \sigma_1^2)\mathbf{I})$ and N_{1e}^n is independent of Y_1^n and (M_1, M_2). Therefore, applying EPI as described in (111), we have

$$e^{\frac{2}{n}h(Z^n|M_1,M_2)} \geq e^{\frac{2}{n}h(Y_1^n|M_1,M_2)} + e^{\frac{2}{n}h(N_{1e}^n)}.$$

That is,

$$e^{\frac{2}{n}h(Z^n|M_1,M_2)} \geq e^{\frac{2}{n}[h(Y_1^n|M_1,M_2)-h(Z^n|M_1,M_2)]} \cdot e^{\frac{2}{n}h(Z^n|M_1,M_2)} + e^{\frac{2}{n}h(N_{1e}^n)}.$$

Replacing $h(Y_1^n|M_1, M_2) - h(Z^n|M_1, M_2)$ by its realization as specified in (37) and $h(N_{1e}^n)$ by

$$h(N_{1e}^n) = \frac{n}{2}\log 2\pi e(\sigma_e^2 - \sigma_1^2),$$

we obtain

$$e^{\frac{2}{n}h(Z^n|M_1,M_2)} \geq \frac{\gamma\alpha P + \sigma_1^2}{\gamma\alpha P + \sigma_e^2} e^{\frac{2}{n}h(Z^n|M_1,M_2)} + 2\pi e(\sigma_e^2 - \sigma_1^2).$$

Easy calculation gives

$$h(Z^n|M_1, M_2) \geq \frac{n}{2}\log 2\pi e(\gamma\alpha P + \sigma_e^2).$$

i.e., (38). This concludes our proof.

Appendix J
Proof of Corollary 13

Proof: The upper bound on R_2 remains the same to (31); while the upper bounds on R_1 and $R_1 + R_2$ are obtained by combining (30) and (31). In more details, we have

$$\begin{aligned}
R_1 \overset{(a)}{\leq} & C\left(\frac{\alpha(1-\gamma)P}{\gamma\alpha P + \sigma_1^2}\right) - C\left(\frac{\alpha(1-\gamma)P}{\gamma\alpha P + \sigma_e^2}\right) + R_2 \\
\leq & C\left(\frac{\alpha P}{\sigma_1^2}\right) - C\left(\frac{\alpha P}{\sigma_e^2}\right) + R_2 \\
\overset{(b)}{\leq} & C\left(\frac{\alpha P}{\sigma_1^2}\right) - C\left(\frac{\alpha P}{\sigma_e^2}\right) + C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_2^2}\right) - C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_e^2}\right)
\end{aligned}$$

where (a) is according to (30); (b) is via replacing R_2 by its upper bound as given in (31).

On the other hand, according to (30), we have

$$\begin{aligned} R_1 &\le C\left(\frac{\alpha(1-\gamma)P}{\gamma\alpha P+\sigma_1^2}\right) - C\left(\frac{\alpha(1-\gamma)P}{\gamma\alpha P+\sigma_e^2}\right) + C\left(\frac{(1-\gamma\alpha)P}{\gamma\alpha P+\sigma_e^2}\right) \\ &= C\left(\frac{\alpha(1-\gamma)P}{\gamma\alpha P+\sigma_1^2}\right) + C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_e^2}\right) \\ &\le C\left(\frac{\alpha P}{\sigma_1^2}\right) + C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_e^2}\right). \end{aligned}$$

Summing it up with R_2 which is upper bounded by (31), we get the desired upper bound on R_1+R_2. This concludes our proof. ■

Appendix K
Proof of Theorem 16

Proof: Consider the gap between the inner and outer bounds as specified in (41) and (40), respectively. If we take the same choice of α in both bounds, the gap may occur only in the R_1+R_2 term that is upper bounded by

$$\left[C\left(\frac{\alpha P}{\sigma_1^2}\right) + C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_2^2}\right)\right] - \left[C\left(\frac{\alpha P}{\sigma_1^2}\right) - C\left(\frac{\alpha P}{\sigma_e^2}\right) + C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_2^2}\right)\right] = C\left(\frac{\alpha P}{\sigma_e^2}\right).$$

A first observation is that both bounds coincide at $\alpha=0$. Furthermore, we consider their subregions in the following two cases for comparison.

- Consider the case as $R_2 \le C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_e^2}\right)$. The corresponding subregions of (R_1,R_2) in the inner and outer bound are the same, i.e.,

$$\begin{aligned} R_1 &\le C\left(\frac{\alpha P}{\sigma_1^2}\right) - C\left(\frac{\alpha P}{\sigma_e^2}\right) + C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_2^2}\right) - C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_e^2}\right) \\ R_2 &\le \min\left\{C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_e^2}\right), C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_2^2}\right) - C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_e^2}\right)\right\} \end{aligned}$$

- Consider the other case as $C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_e^2}\right) < R_2 \le C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_2^2}\right) - C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_e^2}\right)$. Note that this case is possible only if

$$C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_e^2}\right) < C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_2^2}\right) - C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_e^2}\right). \tag{112}$$

The above inequality holds for

$$0<\alpha<1 \quad \text{as} \quad \sigma_e^2 \ge P+2\sigma_2^2; \tag{113}$$

or

$$0<\alpha<\frac{(\sigma_e^2-\sigma_2^2)^2}{P(P+\sigma_2^2)} - \frac{\sigma_2^2}{P} \quad \text{as} \quad \sigma_e^2 \le P+2\sigma_2^2. \tag{114}$$

(The calculation of (113) and (114) is similar to the one given in Appendix L.)

Recall that the gap occurs only in the R_1+R_2 term that is upper bounded by $C(\frac{\alpha P}{\sigma_e^2})$. More specifically,

1) as $\sigma_e^2 \ge P+2\sigma_2^2$, we have for $0<\alpha<1$,

$$C\left(\frac{\alpha P}{\sigma_e^2}\right) \overset{(a)}{<} C\left(\frac{P}{\sigma_e^2}\right) \overset{(b)}{\le} C\left(\frac{P}{P+2\sigma_2^2}\right) \le C(1) = 0.5$$

where (a) is by the fact that $C(x)$ is an increasing function with respect to x and α is upper bounded by 1; (b) is due to the fact that $\sigma_e^2 \geq P + 2\sigma_2^2$.

2) as $\sigma_e^2 \leq P + 2\sigma_2^2$, we have for $0 < \alpha < \frac{(\sigma_e^2-\sigma_2^2)^2}{P(P+\sigma_2^2)} - \frac{\sigma_2^2}{P}$,

$$C\left(\frac{\alpha P}{\sigma_e^2}\right) \overset{(c)}{<} C\left(\frac{\sigma_e^2-\sigma_2^2}{P+\sigma_2^2} - \frac{\sigma_2^2(P+\sigma_e^2)}{\sigma_e^2(P+\sigma_2^2)}\right) \overset{(d)}{\leq} C\left(1 - \frac{\sigma_2^2(P+\sigma_e^2)}{\sigma_e^2(P+\sigma_2^2)}\right) \leq C(1) = 0.5$$

where (c) is by the fact that $C(x)$ is an increasing function with respect to x and α is upper bounded by $\frac{(\sigma_e^2-\sigma_2^2)^2}{P(P+\sigma_2^2)} - \frac{\sigma_2^2}{P}$; (d) is due to the fact that $(\sigma_e^2 - \sigma_2^2)/(P + \sigma_2^2) \leq 1$ since $\sigma_e^2 \leq P + 2\sigma_2^2$.

This concludes our proof. ■

Appendix L
Calculation for (42)

To find α such that (42) holds, we consider

$$C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_2^2}\right) - 2C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_e^2}\right) \leq 0$$

which is equivalent to having

$$\frac{1}{2}\log\frac{(P+\sigma_2^2)(\alpha P+\sigma_e^2)^2}{(\alpha P+\sigma_2^2)(P+\sigma_e^2)^2} \leq 0, \quad \text{i.e.,} \quad \frac{(P+\sigma_2^2)}{(P+\sigma_e^2)^2}(\alpha P+\sigma_e^2)^2 \leq (\alpha P+\sigma_e^2) - (\sigma_e^2-\sigma_2^2).$$

Note that this inequality can be formulated as a quadratic inequality with respect to $\alpha P + \sigma_e^2$. Accordingly, denoting $x = \alpha P + \sigma_e^2$, $A = \frac{(P+\sigma_2^2)}{(P+\sigma_e^2)^2}$, and $C = \sigma_e^2 - \sigma_2^2$, we represent the inequality above by $f(x) = Ax^2 - x + C \leq 0$. Here, as $A \geq 0$, $f(x)$ is convex and this inequality holds when

$$\frac{1-T}{2A} \leq x \leq \frac{1+T}{2A}, \quad \text{where} \quad T = \sqrt{1-4AC} = \frac{P+2\sigma_2^2-\sigma_e^2}{P+\sigma_e^2}.$$

Here, $T \geq 0$ as the assumptions in the theorem implies that $P \geq \frac{\sigma_e^2}{\sigma_2^2}(\sigma_e^2 - 2\sigma_2^2) \geq (\sigma_e^2 - 2\sigma_2^2)$, where the last inequality is due to $\sigma_e^2 \geq \sigma_2^2$. Using the values of T, A, and x in this last condition, we obtain that $f(x) \geq 0$ if and only if

$$\frac{(\sigma_e^2-\sigma_2^2)^2}{P(P+\sigma_2^2)} - \frac{\sigma_2^2}{P} \leq \alpha \leq 1.$$

References

[1] T. Cover, "Broadcast channels," *IEEE Trans. Inf. Theory*, vol. 18, no. 1, pp. 2–14, Jan. 1972.

[2] P. Bergmans, "Random coding theorem for broadcast channels with degraded components," *IEEE Trans. Inf. Theory*, vol. 19, no. 2, pp. 197–207, Mar. 1973.

[3] R. G. Gallager, "Coding and capacity for degraded broadcast channels," *Problemy Peridachi Informatsi*, vol. 10, no. 3, pp. 3–14, 1974.

[4] R. Ahlswede and J. Körner, "Source coding with side information and a converse for degraded broadcast channels," *IEEE Trans. Inf. Theory*, vol. 21, no. 6, pp. 629–637, Jun. 1975.

[5] K. Marton, "A coding theorem for the discrete memoryless broadcast channel," *IEEE Trans. Inf. Theory*, vol. 25, no. 3, pp. 306–311, May 1979.

[6] A. El Gamal and E. Van Der Meulen, "A proof of Marton's coding theorem for the discrete memoryless broadcast channel (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 27, no. 1, pp. 120–122, Jan. 1981.

[7] E. Ekrem and S. Ulukus, "Secrecy capacity of a class of broadcast channels with an eavesdropper," *EURASIP Journal on Wireless Communications and Networking*, Jan. 2009. [Online]. Available: http://jwcn.eurasipjournals.com/content/2009/1/824235

[8] C. Nair and A. El Gamal, "The capacity region of a class of three-receiver broadcast channels with degraded message sets," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4479–4493, Oct. 2009.

[9] Y.-K. Chia and A. El Gamal, "Three-receiver broadcast channels with common and confidential messages," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 2748–2765, May 2012.

[10] E. Ekrem and S. Ulukus, "Multi-receiver wiretap channel with public and confidential messages," *IEEE Trans. Inf. Theory*, vol. 59, no. 4, pp. 2165–2177, Apr. 2013.

[11] Y. Chen, O. O. Koyluoglu, and A. Sezgin, "On the achievable individual-secrecy rate region for broadcast channels with receiver side information," in *Proc. 2014 IEEE International Symposium on Information Theory (ISIT 2014)*, Jun. 2014, pp. 26–30.

[12] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, 1949.

[13] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[14] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[15] A. Carleial and M. Hellman, "A note on Wyner's wiretap channel (Corresp.)," *IEEE Trans. Inf. Theory*, vol. 23, no. 3, pp. 387–390, May 1977.

[16] J. Körner and K. Marton, "General broadcast channels with degraded message sets," *IEEE Trans. Inf. Theory*, vol. 23, no. 1, pp. 60–64, Jan. 1977.

[17] S. Diggavi and D. Tse, "On opportunistic codes and broadcast codes with degraded message sets," in *Proc. 2006 IEEE Information Theory Workshop (ITW 2006)*, Mar. 2006, pp. 227–231.

[18] C. Nair and Z. Wang, "On 3-receiver broadcast channels with 2-degraded message sets," in *Proc. 2009 International Symposium on Information Theory (ISIT 2009)*, Jun. 2009, pp. 1844–1848.

[19] A. E. Gamal and Y.-H. Kim, *Network Information Theory*. New York, NY, USA: Cambridge University Press, 2012.

[20] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.

[21] ——, "Degraded compound multi-receiver wiretap channels," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 5681–5698, Sep. 2012.

[22] Y. Chen, O. O. Koyluoglu, and A. Sezgin, "On the individual secrecy rate region for the broadcast channel with an external eavesdropper," in *Proc. 2015 IEEE International Symposium on Information Theory (ISIT 2015)*, Jun. 2015, pp. 1347–1351.

[23] N. Cai and K. Lam, "How to broadcast privacy: Secret coding for deterministic broadcast channels," in *Numbers, Information and Complexity*, I. Althöfer, N. Cai, G. Dueck, L. Khachatrian, M. Pinsker, A. Sárközy, I. Wegener, and Z. Zhang, Eds. Springer US, 2000, pp. 353–368.

[24] R. Liu, I. Maric, P. Spasojević, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[25] Z. Goldfeld, G. Kramer, and H. H. Permuter, "Broadcast channels with privacy leakage constraints," *CoRR*, vol. abs/1504.06136, Apr. 2015. [Online]. Available: http://arxiv.org/abs/1504.06136

[26] O. O. Koyluoglu, Y. Chen, and A. Sezgin, "Broadcast channel with receiver side information: Achieving individual secrecy," in *Proc. 2014 International Zurich Seminar on Communications (IZS 2014)*, Zurich, Switzerland, Feb. 2014.

[27] Y. Chen, O. O. Koyluoglu, and A. Sezgin, "Individual secrecy for broadcast channels with receiver side information," *CoRR*, vol. abs/1501.07547, Jan. 2015. [Online]. Available: http://arxiv.org/abs/1501.07547

[28] R. Wyrembelski, A. Sezgin, and H. Boche, "Secrecy in broadcast channels with receiver side information," in *Proc. Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR 2011)*, Nov. 2011, pp. 290–294.

[29] A. S. Mansour, R. F. Schaefer, and H. Boche, "Capacity regions for broadcast channels with degraded message sets

and message cognition under different secrecy constraints," *CoRR*, vol. abs/1501.04490, Jan. 2015. [Online]. Available: http://arxiv.org/abs/1501.04490

[30] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "Secrecy rate region of the broadcast channel with an eavesdropper," *CoRR*, vol. abs/0910.3658, Oct. 2009.

[31] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Apr. 1978.

[32] M. Costa, "A new entropy power inequality," *IEEE Trans. Inf. Theory*, vol. 31, no. 6, pp. 751–760, Nov. 1985.

[33] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, pp. 379–423, Jul. 1948.